

HC5TTUZ1

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

---

V.

15 Cr. 536 (PGG)

KALEIL ISAZA TUZMAN, et al.,

## Defendants

### Trial

New York, N.Y.  
December 5, 2017  
9:40 a.m.

Before:

HON. PAUL G. GARDEPHE,

District Judge  
-and a jury-

## APPEARANCES

JOON H. KIM

Acting United States Attorney for  
the Southern District of New York

A. DAMIAN WILLIAMS

ANDREA M. GRISWOLD

JOSHUA A. NAFTALIS

Assistant United States Attorneys

GIBSON, DUNN & CRUTCHER, LLP

Attorneys for Defendant Isaza Tuzman

AVI WEITZMAN

MARCELLUS A. MCRAE

BOTES, SCHILLER & FLEXNER LLP

Attorneys for Defendant Amanat.

RANDALL W. JACKSON

KINDRED W. CHAKES  
JOANNA C. WRIGHT

SOUTHERN DISTRICT REPORTERS, P.C.  
(212) 905-0300

HC5TTUZ5

DeCapua - Direct

1 FBI, followed by Stephen Maiden.

2 THE COURT: And how long do you anticipate the  
3 testimony to take from the agent and Ms. Amato?

4 MS. GRISWOLD: An hour and a half for the two of them  
5 for direct examination.

6 THE COURT: Okay. I have been told that -- do you  
7 have an idea of how long the cross will be?

8 No idea. Okay. I was told I only have Mr. Maiden  
9 until 6:30 so you know.

10 MS. GRISWOLD: The government calls Special Agent Joel  
11 DeCapua.

12 JOEL DECAPUA,

13 called as a witness by the Government,

14 having been duly sworn, testified as follows:

15 DIRECT EXAMINATION

16 BY MS. GRISWOLD:

17 Q. Where do you currently work?

18 A. I work for the Federal Bureau of Investigation.

19 Q. If I could ask you to speak in the microphone and keep your  
20 voice up, because the acoustics in here aren't great.

21 What is your position with the FBI?

22 A. I'm a special agent.

23 Q. When did you originally join the FBI?

24 A. I joined the FBI August 18, 2009.

25 Q. Briefly, what did you do before you joined the FBI?

HC5TTUZ5

DeCapua - Direct

1 A. Prior to the FBI I worked as a financial investigator for  
2 the State of Indiana.

3 Q. How long did you do that?

4 A. Five years.

5 Q. What squad are you currently assigned to?

6 A. Currently assigned to squad CY2.

7 Q. And what type of squad is that?

8 A. It is a criminal cyber investigation squad.

9 Q. When you use the term criminal in the context of a cyber  
10 squad, does that have any particular meaning?

11 A. It does. We work network intrusions, and we differentiate  
12 the work we do between national security and criminal. The  
13 national security squads will focus on state-sponsored hacking,  
14 and the criminal cyber squads focus on criminal acts.

15 Q. And your squad is a criminal squad?

16 A. That's correct.

17 Q. How long have you been on CY2?

18 A. I have been on CY2 since 2014.

19 Q. And prior to that what squad were you on?

20 A. Prior to that I was in the Newark division, and I worked at  
21 a squad that focused on securities fraud and public corruption.

22 Q. Can you describe for the Court the training you have  
23 received at the FBI in cyber security and digital forensics,  
24 beginning with Quantico?

25 A. So at Quantico every new agent goes through a training

HC5TTUZ5

DeCapua - Direct

1 regimen where we learn about cyber investigations. We learn  
2 how to read email headers, we learn how to resolve IP addresses  
3 and gather evidence as it relates to cyber investigations.

4 From there, every agent receives periodic training about  
5 handling digital evidence and how to investigate various cyber  
6 crimes. When I joined the actual cyber squad, my training went  
7 to a new level and I became more formalized and more in depth.

8 Q. Can you describe what additional or more formal and in  
9 depth training you received, specifically in the cyber security  
10 and digital forensic area, once you joined the cyber squad?

11 A. So the FBI has a training regimen for all cyber agents.  
12 Some of it is self study, some of it is classes that are put  
13 on. Most of my training has been through third-party sources,  
14 in particular an organization known as SANS, and also some  
15 training sponsored by FBI headquarters for digital evidence  
16 handling and forensics called Dex training. DExT.

17 Q. What type of training is Dex training?

18 A. You learn how to collect evidence and analyze evidence as  
19 it relates to digital artifacts that are found on computers.

20 Q. You used the term a moment ago "an email header," I want to  
21 make sure we're defining some of the terms you will use in your  
22 testimony today. What do you mean when you use the term "email  
23 header?"

24 A. When I say "email header" I'm referring to the information  
25 that is transmitted with every single email that you can find

HC5TTUZ5

DeCapua - Direct

1 if you know what to look for. It's the date it was sent, who  
2 it was sent from, who it was sent to, the time it was sent, and  
3 all the stops along the way the email made from the time it  
4 went to the person who was sending the email's computer to  
5 recipient's computer.

6 Q. Is all of that information information that appears on the  
7 face of an email that a normal recipient would obtain?

8 A. So you can't see the header information when you're looking  
9 at a normal email that you might see in Outlook or whatever  
10 email you use. However, there's ways to get behind the scenes  
11 to see the embedded header information.

12 Q. We'll come back to headers in some more detail, but before  
13 we do that I want to ask you about certifications that you hold  
14 that are related to digital forensics. Do you hold any  
15 certifications of this kind?

16 A. Yes, I do.

17 Q. How many do you hold?

18 A. I believe it's seven.

19 Q. And who issued those certifications?

20 A. The certifications were issued by an organization known as  
21 G-I-A-C.

22 Q. What is GIAC?

23 A. GIAC stands for the Global Information Assurance  
24 Certification. And it's a nonprofit organization that sponsors  
25 training and testing and certifications for various cyber

HC5TTUZ5

DeCapua - Direct

1 security and digital forensics trainings.

2 Q. Can you tell the Court the particular certifications that  
3 are relevant to your review of emails in their electronic form?

4 A. I a certified forensic analyst, a certified forensic  
5 examiner, I'm a certified network forensic analyst, and I have  
6 a securities essentials certification from SANS.

7 Q. As a practical matter, how did you obtain these  
8 certifications? What did you have to do to get them?

9 A. I applied to take the third-party sponsored training where  
10 I attended the training course or self studied. Then I made a  
11 reservation for a proctor and I sat for the tests in order to  
12 obtain the certification.

13 Q. When did you receive -- what year to what year did you  
14 receive the certifications that you just testified about that  
15 are relevant to digital forensics?

16 A. Between 2014 and 2017.

17 Q. And in those trainings, in obtaining those certifications,  
18 did that involve the analysis of email headers?

19 A. Yes, it did.

20 Q. Can you describe briefly, some of your recent public cyber  
21 security cases investigations that you have been involved in?

22 A. Yes, I was involved in the 2014 insider hack of Morgan  
23 Stanley, the 2014 hack of JP Morgan Chase, and the 2014 hack of  
24 Scott Trade, and the 2014 hack of E-trade, the 2015 hack of  
25 Cravath and Weil Gotshal, and those are some recent cases that

HC5TTUZ5

DeCapua - Direct

1 are public.

2 Q. When you say you were involved in, were you an  
3 investigating cyber agent on each of those cases?

4 A. Yes, I was heavily involved in each of those cases.

5 Q. Did each of those cases involve the analysis of emails?

6 A. Yes.

7 Q. Are you familiar with the term "web mail?"

8 A. I am.

9 Q. What does it mean?

10 A. Web mail generally means a place that you can go on the  
11 internet to send and receive emails.

12 Q. And during your tenure at the FBI, have you been involved  
13 in reviewing emails received from web mail providers?

14 A. I have.

15 Q. What are the common web mail providers that you are  
16 familiar with?

17 A. There's Google, Google Gmail, Yahoo, Hot Mail, Microsoft.

18 Q. Approximately how many web mail accounts have you been  
19 involved in reviewing during your tenure at the FBI?

20 A. About a hundred.

21 Q. Does that include accounts hosted by Yahoo?

22 A. Yes.

23 Q. Does that include accounts hosted by Microsoft?

24 A. Yes.

25 Q. And in the course of those reviews, did you also have

HC5TTUZ5

DeCapua - Direct

1 occasion to review the header information as part of your  
2 review of the emails?

3 A. In some circumstances, yes.

4 Q. Did you become familiar with typical features of email as  
5 they appear in their electronic format?

6 A. Yes.

7 Q. Has your review included the review of email chains?

8 A. Yes.

9 MS. GRISWOLD: If we could pull up, please, for the  
10 witness what is marked for this hearing only as Government  
11 Exhibit 3553. I have a hard copy for the Court if it would  
12 like.

13 THE COURT: Yes, thank you.

14 Q. Do you see that?

15 A. I do.

16 Q. Did there come a time when the government asked you to take  
17 a look at the email?

18 A. Yes.

19 Q. Approximately when was that?

20 A. It was about two weeks ago.

21 Q. And just for the record, does this appear to be a May 8,  
22 2009 email chain?

23 A. Yes.

24 Q. Based on your initial review of this email and from your  
25 training and experience at the FBI reviewing emails, did you

HC5TTUZ5

DeCapua - Direct

1 observe anything that stood out to you --

2 A. I did.

3 Q. -- as potentially inconsistent?

4 A. Yes, I did.

5 Q. Can you walk the Court through what it is that you --

6 MS. GRISWOLD: And actually if we could zoom out and  
7 go side by side, this page and the next page.

8 Q. I don't think these screens allow you to circle, but could  
9 you identify emails and walk the Court through what you notice  
10 about this email.

11 A. So the first thing that immediately struck me was just some  
12 of the formatting in the email. When I reviewed this, I had  
13 the PDF version, and looking at it, I know the cadence of  
14 emails when you reply and when you forward and reply and  
15 forward, and what I expect to see is on the right-hand side of  
16 the screen are where you see these greater than signs.

17 THE COURT: These what?

18 THE WITNESS: The greater than signs.

19 Q. Is that what is being highlighted?

20 A. Yes.

21 Q. In a normal email chain you will see the responses and the  
22 replies and they will be indented like this by the email  
23 service when you actually do the reply. This email, it has  
24 this format up until it's the May 8, 2009 at 5:05 p.m. email,  
25 then after that the formatting changes to something that I

HC5TTUZ5

DeCapua - Direct

1 don't recognize where everything is kind of in line with these  
2 lines on the top and the from and sent to, they have asterisks  
3 on the outside of them. I would expect this email to have a  
4 consistent format if it were authentic.

5 Should I continue?

6 Q. Yes.

7 What, if any, other features did you notice?

8 A. Something else that struck me is the time zone difference  
9 between the May 8, 2009 at 5:27 p.m. Eastern Standard Time  
10 email and the May 8, 2009, 5:21 p.m. Eastern Daylight Savings  
11 Time email.

12 Q. So you're comparing these two, the one on the left-hand  
13 side?

14 A. Yes.

15 Q. Why did that strike you?

16 A. I expect them to be consistent because it was on the same  
17 day. I don't know if there's anywhere in the world where one  
18 place is Eastern Standard Time and the other is Eastern  
19 Daylight Time at the same time. I believe May 8 is Eastern  
20 Daylight Time.

21 Q. So is it fair to say this is just one factor that struck,  
22 not determinative of anything?

23 A. No, it's just something that I noticed as strange.

24 Q. What, if anything else, about this email stood out to you?

25 If we could go to the very last page.

HC5TTUZ5

DeCapua - Direct

1 A. If you go to the last page, you see the formatting above  
2 the final footer, and it's all the greater than signs, and  
3 that's part of the chain that I said looked normal.

4 But then right below it, I see there's a footer, like  
5 the sender signature, which I would expect to see, but it's  
6 weird because when you look at the email address of it, it's  
7 Kaleil at kpcapital.com, but some of the emails way later in  
8 the chain, you see that outside the greater than signs, if you  
9 could go up to first page you see that Kaleil email address  
10 that's used here is kit@kitcapital.com, and I thought that was  
11 interesting, because it wasn't from kpcapital.com. Another  
12 anomaly, something that I thought was strange.

13 And one other thing, if you look at the subject line  
14 of the May 8, 2009 at 5:21 p.m. email, the subject line --

15 THE COURT: What was the time?

16 THE WITNESS: The 5:21 p.m. Eastern Daylight Time  
17 email, the subject line doesn't say re or forward or anything  
18 that I would expect it to say if it was reply or a forward  
19 email, which I believe it is, or it's supposed to be. But when  
20 you look at the other subject lines in the chain, they all say  
21 re or forward. That's something else I noticed right off the  
22 bat that struck me as strange.

23 Q. After observing these characteristics, did you suggest any  
24 methods by which the government might investigate the  
25 authenticity of this 5:21 p.m. email?

HC5TTUZ5

DeCapua - Direct

1 A. I did.

2 Q. What did you suggest?

3 A. I suggested that you look at who the email was from,  
4 kit@kitcapital.com, obtain a search warrant for that account,  
5 see if you could find the email in that account, and also  
6 search all the recipient emails to see if the email is one of  
7 those accounts. Because as I explained, emails aren't  
8 self-authenticating, you need to find them in order to  
9 determine whether or not they actually were sent from one  
10 person to another. And if you find them in two accounts, then  
11 it's generally more likely that it's a true email than if it's  
12 just in one account.

13 Q. If we zoom out and go to the very top email that's the from  
14 Chach 786, do you see that email?

15 A. I do.

16 Q. Would you be able to, by getting a search warrant on this  
17 top account, any of the accounts on the top email, can you use  
18 that to authenticate those for emails that come lower in the  
19 chain?

20 A. No.

21 Q. Why not?

22 A. Because if you did a search warrant on say the chach786@aol  
23 account email, it will show what is in that account at this  
24 period of time. And we'll be able to analyze the header  
25 information for that specific email that is from chach785@aol

HC5TTUZ5

DeCapua - Direct

1 but not include any embedded data for any of the prior emails.

2 Q. If we pull back up the 5:21 p.m. email, what is the sender  
3 account of the 5:21 p.m. email as it appears on your screen?

4 A. The sender account is kit@kitcapital.com.

5 Q. Did the government obtain a search warrant for this  
6 account?

7 A. Yes.

8 Q. Were you the agent who obtain the search warrant?

9 A. No.

10 Q. Was the search warrant limited to the three-day time  
11 period, May 7 to 9, 2009?

12 A. Yes.

13 Q. Have you reviewed the results of the search warrant?

14 A. I have.

15 Q. Personally?

16 A. Yes.

17 MS. GRISWOLD: If we could pull up, please, what is  
18 marked for identification as Government Exhibit 3555.

19 Would your Honor like a hard copy?

20 THE COURT: Please.

21 MR. WEITZMAN: May I request that defense counsel get  
22 a hard copy as well?

23 THE COURT: Yes.

24 MS. GRISWOLD: I ask you to give one to Mr. Jackson.

25 Q. Do you recognize what is marked as 3555?

HC5TTUZ5

DeCapua - Direct

1 A. I do.

2 Q. How do you recognize it?

3 A. This is part of a spreadsheet that I created.

4 Q. And is this spreadsheet -- was this created based on your  
5 review of the search warrant returns for the kit@kitcapital.com  
6 account?

7 A. Yes.

8 MS. GRISWOLD: For the purpose of this hearing, the  
9 government offers Government Exhibit 3555.

10 THE COURT: Any objection?

11 MR. JACKSON: No objection.

12 THE COURT: 3555 is received for purposes of hearing.

13 (Government's Exhibit 3555 received in evidence)

14 Q. Now the information in the left most column, what is  
15 contained in that column?

16 A. In the left most column are the numbered emails of the  
17 thread of the email PDF that you provided to me. And each one  
18 contains the date that that email was sent, according to the  
19 face of the email, and who it was from.

20 Q. Putting this aside next to 3553, for example, if we look at  
21 what is indicated here as email 7, 5/8/2009 at 5:21 at  
22 Government Exhibit 3555, does that relate to what we're seeing  
23 on the right side of the screen from 3553?

24 A. Yes.

25 Q. So walk the Court through what this chart reflects in terms

HC5TTUZ5

DeCapua - Direct

1 of your review of the search warrant returns for the  
2 kit@kitcapital.com account.

3 A. So as I said before, one of the ways I suggested to verify  
4 the authenticity of this email is to search the sender's  
5 account. And after we received the sender's account, I looked  
6 to find the this email, email number 7, and it wasn't in there.

7 But in order to verify that we received all the emails  
8 from that time period, we also looked at all the preceding  
9 emails in the email chain, and those are the ones numbered one  
10 through six. And in reviewing the kit@kitcapital account, I  
11 found each one of those emails in the account somewhere, and  
12 also email eight, which is an email after email seven, but I  
13 did not find email seven anywhere in the account.

14 Q. You said that you -- also there's an email in asterisks --

15 THE COURT: You may want to talk a little more  
16 directly into the microphone.

17 MS. GRISWOLD: Sorry, your Honor.

18 Q. So you were able to find each of the emails that appear in  
19 Government Exhibit 3553 in the kit@kitcapital.com search  
20 warrant results with the exception of the 5:21 p.m. email. Is  
21 that an accurate summary?

22 A. Yes.

23 Q. And you found one additional email in this email chain. Is  
24 that what email eight reflects?

25 A. Yes, with the same subject line and everything.

HC5TTUZ5

DeCapua - Direct

1 Q. I want to show you Government Exhibit 1589, if we could  
2 pull that up, it's in evidence at the trial. Is this the May  
3 8, 2009 email with the same subject line?

4 A. Yes.

5 Q. I want to direct your attention to the email from Stephen  
6 Maiden to a number of different recipients at 11:47. Do you  
7 see that?

8 A. I do.

9 Q. Is this one of the emails that you looked for in the  
10 kit@kitcapital.com account?

11 A. I think so, yes.

12 MS. GRISWOLD: If we could pull in side by side with  
13 chart 3555 so we could be sure.

14 If you could highlight email number three, please.

15 Q. Is this the email that you looked for, 7:47, and indicated  
16 as 11:47 in the other exhibit?

17 A. Yes, and the difference is due to time zones.

18 Q. In the email that's in evidence as Government Exhibit 1589,  
19 do you see a recipient Irfan Amanat on this email?

20 A. Yes.

21 Q. What is the email address that Mr. Irfan Amanat received  
22 the email?

23 A. Irfan.amanat@gmail.com.

24 Q. Going back to Government Exhibit 3555 --

25 MS. GRISWOLD: Put that back up again, May 8, 2009

HC5TTUZ5

DeCapua - Direct

1 printed chain and start 3553.

2 Q. Looking at the email chain, did you review it to see if  
3 Irfan Amanat was copied on each of these emails from the  
4 5:21 p.m. email below?

5 A. Yes.

6 Q. And based on your review, did you identify any email  
7 address other than the irfan.amanat@gmail.com?

8 MR. JACKSON: Objection, your Honor, I don't  
9 understand the question.

10 THE COURT: I don't understand.

11 MS. GRISWOLD: I'll rephrase it.

12 Q. The 5:21 p.m. email, does it indicate the email address  
13 that Mr. Irfan Amanat received this email at?

14 A. No.

15 Q. Did you review the kit@kitcapital.com search warrant  
16 results for emails during the three-day period to and from  
17 Irfan Amanat?

18 A. Yes.

19 Q. Did you find some?

20 A. Yes.

21 Q. Approximately how many emails did you find between the  
22 kit@kitcapital.com account and Irfan Amanat?

23 A. There was about ten.

24 Q. What email address did Irfan Amanat receive or send those  
25 emails to and from?

HC5TTUZ5

DeCapua - Direct

1 A. The gmail account.

2 Q. Did you find evidence that the kit@kitcapital.com account  
3 ever sent an email to another Irfan Amanat account?

4 A. I didn't see it in the email search warrant return, no.

5 MR. JACKSON: Your Honor, I'm just going to make -- I  
6 don't want to delay things, but I'm making I generalized  
7 leading objection because it's hard for me to follow without  
8 getting a non-leading answer from the witness. That's my  
9 objection going forward.

10 THE COURT: I haven't observed any leading. I'm not  
11 really sure what you're asking for. It sounds like you're not  
12 understanding the testimony, is that what you're saying?

13 MR. JACKSON: It's fine, your Honor, I was previewing  
14 that I may make an objection. I think we're close to leading,  
15 but --

16 THE COURT: Okay.

17 MS. GRISWOLD: We could take that down.

18 Q. You testified earlier briefly about the concept of header  
19 information. Is that sometimes will also referred to as  
20 metadata?

21 A. Yes.

22 Q. Are you familiar with what is known as a message ID within  
23 a header?

24 A. Yes.

25 Q. Describe what that is.

HC5TTUZ5

DeCapua - Direct

1 A. So in the header information are a variety of different  
2 fields that the typical user wouldn't see. But when you open  
3 up an email's header, one of the fields is something called  
4 message ID. And a message ID is something that is attached to  
5 an email by the software that sends it. So if it's your home  
6 computer, it's going to be Outlook or Apple mail that attaches  
7 the message ID. If you use gmail or AOL it will be the email  
8 sever hosted by those companies that attaches the message ID.  
9 When it's created, the message ID is a random -- it has to be a  
10 random number, a completely unique number, and --

11 Q. But what you can tell from it is the software from which it  
12 was sent, is that your testimony?

13 A. Yeah. So like I said, the message ID only has to be  
14 unique, but there are certain patterns that you observe where  
15 certain software's message ID always looks the same, and it's  
16 generally agreed upon and accepted that you can look at a  
17 message --

18 MR. JACKSON: Objection, generally agreed upon.

19 THE COURT: Overruled.

20 A. I can look at a message ID and determine in some  
21 circumstances what software was used to send the email.

22 Q. Let's get more specific. Going back to your review of the  
23 kit@kitcapital.com search warrant results from period May 7 to  
24 May 9, 2009, did you go through and review the message ID for  
25 emails sent from this account during that three-day period?

HC5TTUZ5

DeCapua - Direct

1 A. Yes, I did.

2 MS. GRISWOLD: I want to put up for the witness what  
3 is marked as Government Exhibit 3556.

4 THE COURT: Don't feel like you have to rush, we'll  
5 take as long as we need.

6 Q. Do you recognize what is marked as Government Exhibit 3556?

7 A. Yes, I do.

8 Q. How do you recognize it?

9 A. I created it.

10 Q. And did you create it based on your review of the  
11 kit@kitcapital.com search warrant results?

12 A. Yes.

13 MS. GRISWOLD: The government offers Government  
14 Exhibit 3556 for the purpose of this hearing.

15 THE COURT: Any objection?

16 MR. JACKSON: No objection, your Honor.

17 THE COURT: Government Exhibit 3556 is received for  
18 the purposes of hearing.

19 (Government's Exhibit 3556 received in evidence)

20 Q. Let's start with the title, it says selected header data  
21 from email sent by kit@kitcapital.com, and then it indicates  
22 Microsoft search warrant return and May 8, 2009 email provided  
23 by defendant. Do you see that?

24 A. I do.

25 Q. So for all -- I want to first focus on all of the rows with

HC5TTUZ5

DeCapua - Direct

1 the exception of the highlighted one. Is the information  
2 contained in -- tell us where you got the information for all  
3 of the rows, putting aside the highlighted row.

4 A. The first thing I did is -- in the search warrant return I  
5 looked at all the emails that were sent by kit@kitcapital.com,  
6 and then I looked at the header information for each one of  
7 those emails, and every single email here represents an email  
8 that I found that was sent by kit@kitcapital.com for that  
9 three-day period.

10 For each one of those I pulled out the time it was  
11 sent, who it was sent from, the subject line, and then the  
12 message ID, which I explained to you earlier. And this chart  
13 presents these in chronological order from the very first email  
14 sent from kit@kitcapital.com all the way to the very last one  
15 in the search warrant return, which was May 9.

16 Q. And again, putting aside the highlighted one, was there any  
17 common characteristic within the message ID that you were able  
18 to see from your review of all of the message IDs in the sent  
19 emails?

20 A. Yes, they were all consistent, they had a consistent  
21 format, which told me that the messages were -- the emails were  
22 sent by the same either client side email service or the same  
23 web mail service. And in this case, you see the seemingly  
24 random unique identifier, and then it is -- after this unique  
25 identifier is a domain name, which I looked up the domain name

HC5TTUZ5

DeCapua - Direct

1 it's a -- MI8 is a company based out of New York that handled  
2 web mail services for Blackberries and other mobile devices.

3 Q. So all of these say MI8 on them, with the exception of  
4 highlighted one?

5 A. That is correct.

6 Q. What does that tell you?

7 A. It tells me that all the emails, with the exception of the  
8 highlighted one, were sent from the same device.

9 MS. GRISWOLD: If we keep that up and put next to it  
10 what is marked as Government Exhibit 3549, and I will pass up a  
11 copy for the Court.

12 Q. Are you familiar with Government Exhibit 3549 on your  
13 screen?

14 A. Yes.

15 Q. What is Government Exhibit 3549?

16 A. This is the May 8, 2009 email that is in question, but it  
17 includes the content and the header information.

18 Q. And was it your understanding this was what was provided to  
19 the defendant when the request was made for the header  
20 information?

21 A. It was.

22 Q. Sorry, provided by the defendant to the government.

23 A. Yes.

24 MS. GRISWOLD: If we could highlight the message ID,  
25 please, and just zoom that out.

HC5TTUZ5

DeCapua - Direct

1 Q. Is the information contained in 3556 information that you  
2 got from Government Exhibit 3549?

3 A. Yes, the highlighted part is.

4 Q. And what did you notice about the message ID in the  
5 metadata of the email provided by the defendant?

6 A. The message ID was inconsistent with the other message IDs  
7 for the emails sent in that time period.

8 Q. How was it inconsistent?

9 A. You can just look at it and see the inconsistencies. It's  
10 a string that first it says at the end kitcapital.com instead  
11 of MI8, and secondly, has a different number of characters and  
12 the characters are separated by dashes.

13 MR. JACKSON: Your Honor, for the record, I'm noting  
14 an objection here, but we'll deal with it later. I think this  
15 is misleading testimony. I'm objecting.

16 THE COURT: Well, I don't understand the basis for  
17 your objection.

18 MR. JACKSON: The witness can't testify that it's  
19 inconsistent when it's his own testimony this is a message ID  
20 indicating a different device. There's nothing inconsistent.

21 THE COURT: I mean he's explaining why the message ID  
22 is different, it looks different on Government Exhibit 3556.  
23 You're welcome to attack it on cross-examination, but we'll  
24 proceed.

25 MR. JACKSON: Thank you, Judge.

HC5TTUZ5

DeCapua - Direct

1 Q. If we could for one more minute pick up 3559, the  
2 highlighted row, that message, were you able to determine what  
3 type of software device is affiliated with the message ID that  
4 appears in the highlighted row?

5 A. Yes, Apple mail.

6 Q. Are you familiar with what is known as a local email  
7 client?

8 A. Yes.

9 Q. What is it?

10 A. A local email client is a piece of software that you have  
11 on your computer that allows you to interact with an email  
12 sever that is on the internet where you can use it to send  
13 emails, receive emails. Some common examples are Outlook and  
14 Thunderbird and Apple mail.

15 Q. In the course of your work as an FBI agent, have you had  
16 experience reviewing emails contained in local email client  
17 accounts?

18 A. I have.

19 Q. Including Outlook?

20 A. Yes.

21 Q. Including Apple mail?

22 A. Yes.

23 Q. In what context have you had the experience to review  
24 those?

25 A. Physical search warrants when we receive someone's hard

HC5TTUZ5

DeCapua - Direct

1 drive or physical computer, sometimes we can obtain the emails  
2 that they send or receive by analyzing the local email client  
3 on that machine.

4 Q. And in your experience, are you able to pull emails from a  
5 web mail account such as Yahoo onto a local email client such  
6 as Outlook or Apple mail?

7 A. Yes.

8 Q. How do you access a web mail account such as Yahoo through  
9 a local client account?

10 A. It's usually very simple, you just click add account.

11 Sometimes when you open the software for the first time it will  
12 ask you let's set up an account where you would input your  
13 email address.

14 Q. Just to be clear, when you say when you set up, what are  
15 you in? Talking within the local email client?

16 A. Yeah, within the local email client application.

17 Q. So go on a computer and you go into Outlook or Apple mail?

18 A. That's correct. And it prompts you enter your email  
19 address and password.

20 Q. I would like to pull up what is marked for identification  
21 as Government Exhibit 2908. Does this appear to be a June 14,  
22 2008 email exchange between an Omar Amanat and Irfan Amanat?

23 A. Yes.

24 Q. Was this provided to you in the context of your testimony  
25 today by the government?

HC5TTUZ5

DeCapua - Direct

1 A. It was.

2 MS. GRISWOLD: For the purposes of this hearing, the  
3 government offers Government Exhibit 2908.

4 THE COURT: Any objection?

5 MR. JACKSON: No objection, your Honor.

6 THE COURT: 2908 is received.

7 (Government's Exhibit 2908 received in evidence)

8 MS. GRISWOLD: To note for the Court, this was an  
9 email that was produced by Google in response to a search  
10 warrant on the Irfan Amanat @gmail.com account.

11 Q. When was the first time you were shown this email?

12 A. Maybe a week ago.

13 Q. I want to direct your attention to the email at 2205 from  
14 the account omar@amanatcapital.com. Do you see that?

15 A. I do.

16 Q. Who is that email to?

17 A. It's to irfan.amanat@gmail.com.

18 Q. Can you read what Mr. Amanat, Omar Amanat, wrote to Irfan  
19 Amanat in this email?

20 A. Hey Iffi, I also want to delete all of my emails from the  
21 Yahoo site but download them onto my laptop. How can I do  
22 this? I'm concerned about them subpoenaing Yahoo at some  
23 point.

24 Q. And if you could go to the email at 2321, and if you  
25 could please read Mr. Irfan Amanat's response at 2321.

HC5TTUZ5

DeCapua - Direct

1 A. Set up your Outlook to pull all your email from Yahoo and  
2 delete it. If you need help I can walk you through it.

3 Q. So you testified that in your experience as an FBI agent  
4 you're familiar with how to pull emails from a web mail account  
5 such as Yahoo onto a local client account?

6 A. Yes.

7 Q. Do you need any special FBI or proprietary software of any  
8 kind to do that?

9 A. No.

10 Q. What do you use to do that?

11 A. You can use Apple mail, you can use Thunderbird, you can  
12 use Outlook.

13 Q. In preparation for your testimony today, did you create one  
14 or more web mail accounts to use to demonstrate for the Court  
15 the interplay between a web mail account and a local client  
16 account?

17 A. I did.

18 Q. Is [janesmith53490@yahoo.com](mailto:janesmith53490@yahoo.com) one of those accounts?

19 A. Yes.

20 Q. And to create this account you went to [yahoo.com](http://yahoo.com)?

21 A. That's correct.

22 MS. GRISWOLD: Your Honor, we have an FBI computer  
23 here that we would like to hook up so that your Honor can see.

24 THE COURT: Okay. How about the defense?

25 MS. GRISWOLD: Oh, yes, the defense as well.

HC5TTUZ5

DeCapua - Direct

1 MR. JACKSON: Your Honor, may I request that we have  
2 the spelling of the name again of that account, Jane Smith.

3 MS. GRISWOLD: Sure, it's Jane Smith with no spaces,  
4 53490@yahoo.com.

5 MR. JACKSON: Thank you.

6 Q. Is that your FBI Apple computer that's now populated to the  
7 screen in front of you?

8 A. Yes.

9 Q. Can you please go to -- do you have a hot spot up there so  
10 you're able to connect to the internet?

11 A. Yes.

12 Q. Can you please go to yahoo.com and log into the Jane Smith  
13 account that I just put on the record.

14 When did you create this account?

15 A. It was over the weekend.

16 Q. Do you have a local email client on that laptop?

17 A. I do.

18 Q. What do you have?

19 A. Apple mail.

20 Q. Is there an email in the inbox that you put in this account  
21 for the purpose of this demonstration?

22 A. Yes, you emailed me.

23 Q. Could you pull up that email.

24 So we're at yahoo.com right now, correct?

25 A. That's correct.

HC5TTUZ5

DeCapua - Direct

1 Q. And can you show the Court how you view the header  
2 information once you're actually in the web mail account.

3 A. Yes, once you're in the account, the header information can  
4 be accessed by clicking on this thing that says more, and then  
5 you go down to where it says view raw message, and this is an  
6 example of a header information of an email.

7 Q. And if we could ask you to scroll down and show the message  
8 ID.

9 A. Right here is the message ID.

10 Q. And this indicates that it was sent from what kind of  
11 device? It says usa.doj.gov.

12 A. I don't know what kind of device, but it was behind a DOJ  
13 sever.

14 Q. So can you show the Court how you're able to pull this  
15 email out of the web mail account onto the local email client  
16 account on the computer?

17 A. Certainly.

18 Q. If you could narrate step by step what you're doing in case  
19 the Court wants to inquire.

20 A. Certainly. So the first step is open up Apple mail, and  
21 it's going to ask me to input an email address, email address  
22 and password.

23 Q. The same password that you used to log in the Yahoo  
24 account?

25 A. Yeah, same password. When I click create, it reaches out

HC5TTUZ5

DeCapua - Direct

1 to Yahoo servers, authenticates it's the correct password, and  
2 then begins exchanging information.

3 So that's if anything looks good and ready to go, I  
4 just select the default values and click create.

5 Q. What is appearing on the screen right now? Is this Apple  
6 mail?

7 A. This is Apple mail, and this is what the inbox looks like  
8 to an Apple mail user. And here you will see it has made an  
9 outgoing connection to the Yahoo email server and pulled down  
10 the email. So the email now exists in two places, the Apple  
11 server and this computer in front of me.

12 (Continued on next page)

13

14

15

16

17

18

19

20

21

22

23

24

25

Hc5Wtuz6

DeCapua - Direct

1 BY MS. GRISWOLD:

2 Q. Can you open up the email?

3 So it now exists in both places, you said?

4 A. Yes.

5 Q. Now that you've pulled it down, can you go back to the  
6 Yahoo account and delete it from the Yahoo account so it  
7 doesn't appear there at all?

8 A. I can, but first I'd recommend to export it onto the  
9 desktop.

10 Q. You pull it onto your computer first?

11 A. Yes, pull it on so I know where it is on my computer.

12 Q. Go ahead and do that, and narrate any steps you're taking.

13 A. So, to pull it onto my computer, I would go to mailbox and  
14 I would select "export mailbox." And it's going to ask me  
15 where I want to put it, so I just pick right on my desktop.

16 Now, I go to my desktop to look and check. I see this new  
17 file that's created that says "inbox.mbox," and inside of that,  
18 I see several files, including something called "mbox," which  
19 is going to contain the actual content of my entire inbox that  
20 was loaded into Apple mail.

21 Q. Will that include header information?

22 A. Yes. I can open it for the description.

23 Q. Does it also have the content of the email?

24 A. Yes.

25 Q. OK. Can you now go back into the Yahoo account, please.

Hc5Wtuz6

DeCapua - Direct

1 And if you could delete the email from the account and the  
2 trash folder as well.

3 A. So, I select it, click "delete" and then go to the trash  
4 folder, select all the emails in it and click "delete."

5 There was an earlier test email that I forgot to delete out  
6 of the trash, but I'll do that at this time.

7 Now there should be no emails in the inbox, no emails in  
8 the trash and no emails on Yahoo servers.

9 Q. Based on your experience as an FBI agent and your  
10 involvement in obtaining search warrants, if you were to obtain  
11 a search warrant on this Jane Smith account at this moment in  
12 time, would you expect to get any results?

13 A. I would expect Yahoo to say there's no content available.

14 THE COURT: Yes, we'll take a moment. OK.

15 MS. GRISWOLD: May I?

16 THE COURT: Yes.

17 Q. Now, the email still is on your desktop, correct?

18 A. That's correct.

19 Q. Including the header information?

20 A. Yes, it is.

21 Q. Did you attempt to alter the email and see if you could put  
22 it back in Yahoo in altered form in preparation for your  
23 testimony today?

24 A. I did.

25 Q. Did you need any proprietary tools to do that?

Hc5Wtuz6

DeCapua - Direct

1 A. No.

2 Q. Do you need any special FBI programs?

3 A. No.

4 Q. Did you use anything other than what we've already seen  
5 today?

6 A. No. It was a text editor I used.

7 Q. Can you show the Court in the email that we just had how  
8 you can make changes to the email and then put it back in the  
9 Yahoo account?

10 A. Certainly.

11 For completion, can I delete the email from the local email  
12 client?

13 So, first, I'm going to de-sync the local email client  
14 from the Yahoo account, just so it's not talking to Yahoo  
15 servers and trying to sync itself, and I do that simply by  
16 going into "preferences," selecting Yahoo and clicking the  
17 negative.

18 It's going to ask me if I'm sure I want to remove it. I  
19 do. "Remove." And now there's no emails in the local email  
20 client. However, I know that the email is saved on my desktop.  
21 So, going into the mbox folder, I look at the mbox file and I  
22 double-click it to open it in text editor.

23 Q. Are you able to, for example, change the date on this  
24 email? If it was received Tuesday, December 5, can you change  
25 it to Wednesday, November 15?

Hc5Wtuz6

DeCapua - Direct

1 A. Certainly. To do so, I would just find all the instances  
2 of Tuesday, December 5, and just delete them and type in  
3 whatever date you want.

4 Q. Go ahead and do that. Can you also add yourself to the  
5 email --

6 A. Certainly.

7 Q. -- or make it appear that you've added your email address.

8 THE COURT: You mean as a recipient?

9 MS. GRISWOLD: Yes, your Honor.

10 Q. I think November 15 is the Wednesday.

11 A. I'm sorry.

12 Q. I noticed that you're already copied on this email. Can  
13 you add someone else, perhaps Mr. Naftalis, to the email?

14 A. Yes.

15 These things I'm going to do some copying and pasting.

16 Q. Take your time now. By the way, if you were --

17 I think you missed a T before that Wednesday. Go back up  
18 to the prior one that you did.

19 -- if you were doing this on a PC, what type of  
20 program would you be using?

21 A. Another text editor, like Notepad or Workpad or Microsoft  
22 Word.

23 Q. There's a second 2017.

24 A. And so to add Mr. Naftalis, I would just type his name in,  
25 and then his email address.

Hc5Wtuz6

DeCapua - Direct

1 Q. OK. Can you show us now how you're able to put this back  
2 into the email client account and then Yahoo?

3 A. Once I make my alterations in the text editor, I just save  
4 the file. I go back into the local email client, which is  
5 Yahoo Mail, and I go to "file" -- I'm sorry.

6 It's "file," "import mailboxes," and it's asking me where  
7 am I going to import this data from. I just use an mbox file,  
8 so I'm going to select files in mbox format. I click  
9 "continue," and it asks me to find the mbox. I know it's on my  
10 desktop, and it's inside this folder called inbox.mbox, and I  
11 choose it. From there you can see a new folder has been  
12 populated on Apple Mail, and inside it would be the new email  
13 with the altered --

14 Q. What's the date on this email?

15 A. It's November 15, 2017.

16 Q. And is there an additional recipient?

17 A. The additional recipient -- one moment -- is Mr. Naftalis.

18 Q. And based on -- you tested this in preparation for your  
19 testimony, this process?

20 A. Yes.

21 Q. Is Mr. Naftalis going to actually have an email in his  
22 inbox?

23 A. No.

24 Q. Can you now show us how you put this back into the Yahoo  
25 account?

Hc5Wtuz6

DeCapua - Direct

1 A. Yes. And just to be clear, I could change anything,  
2 including the content and subject line.

3 So, I would re-sync this local email client with the  
4 Yahoo account that I have by going to "mailbox" -- I'm sorry,  
5 "file," "add account." Same process as before, "create," and  
6 as I'm waiting for it to sync, remember that the mailbox is  
7 empty so it won't be doing any syncing right now, but this  
8 folder that I uploaded, I can then take the email that I  
9 created and just drag it to the inbox, and by doing so it makes  
10 an outgoing network connection to Yahoo servers and uploads the  
11 email.

12 Q. Could we go back to the Yahoo.com to the Jane Smith account  
13 now and open up the email that appears there. What is the date  
14 on the email?

15 A. It's November 15.

16 Q. And can you -- and Mr. Naftalis is copied?

17 A. Yes, he is.

18 Q. Can you show the Court where the metadata appears, or the  
19 header information. And again, we're just on Yahoo Mail, on  
20 the Internet right now, correct?

21 A. That's correct. And to be clear, the header doesn't  
22 change.

23 Q. When you say it doesn't change, you mean what? It's the  
24 same as the original, authentic email but with the changes that  
25 you made?

Hc5Wtuz6

DeCapua - Direct

1 A. Yes. So, normally if you were to send an email, forward an  
2 email, the header would always change, but if you upload it  
3 from local email client, as I did right now, the header stays  
4 the same.

5 Q. Did you create a second Yahoo account in connection with  
6 your testimony today?

7 A. I did.

8 Q. Was that SmithJon534@yahoo.com?

9 A. Yes.

10 Q. And was that also created in the last several, in the last  
11 week? When was that account created?

12 A. It was over the weekend.

13 Q. Can you log into that account, please?

14 A. Yes. Before I do, one thing I just want to clarify, the  
15 one thing I found that changes on the header is actually  
16 content length, which is a field that's an undocumented field,  
17 but it looks like it's counting the number of bytes in the  
18 content section of the email, and that's one thing that will  
19 change when I upload it.

20 Q. Now you're logging out of the Jane Smith and into the Jon  
21 Smith account?

22 A. Yeah. I have it saved so I can just click Jon Smith, and  
23 it will automatically log me in, because I was logged in  
24 earlier today.

25 Q. Can we go to the inbox? There are several emails that

Hc5Wtuz6

DeCapua - Direct

1 appear in this inbox, is that correct?

2 A. Yes.

3 Q. Can we go to the one that appears to be dated May 8, 2009.

4 And what does the date and time of this email appear to be?

5 A. It's May 8, 2009, at 5:21 p.m.

6 Q. Who does it appear to be from?

7 A. Kit@kitcapital.com.

8 Q. And what is the content of the email?

9 A. "Also please note that upon execution, all prior agreements  
10 executed in December 2008 by and between KIT, Maiden and Omar  
11 are hereby null and void *ab initio*, and of no further force or  
12 effect from this date forward and going back from inception.

13 Kaleil."

14 Q. We saw earlier in your testimony when we looked at that May  
15 8, 2009, printed email that's marked as Government Exhibit  
16 3553, is the content that we're seeing on the screen the same  
17 content as the 5:21 p.m. email in Government Exhibit 3553?

18 A. The content is, yes.

19 Q. What's different, if anything?

20 A. The recipients.

21 Q. What, if anything, is different about the recipients?

22 A. I added myself and yourself as recipients to this 2009  
23 email.

24 Q. And tell the Court your process for putting this email, the  
25 content of this email in the account, and explain how, if at

Hc5Wtuz6

DeCapua - Direct

1 all, it differed from what you just demonstrated.

2 A. It was essentially the same. I took the PDFs that were  
3 provided of the email metadata and content for the real 5/8,  
4 2009, email and I copied and pasted it into a text document,  
5 and then I uploaded it into my -- before I uploaded, I made  
6 changes to the recipients, and then I uploaded it into Apple  
7 Mail and then synced Apple Mail with this Yahoo account that I  
8 set up.

9 Q. How long did it take you to do that?

10 A. 10 minutes.

11 Q. Can we go to the inbox again, please.

12 I want to show you Government Exhibit -- I'm sorry, Amanat  
13 Exhibit 902, Amanat Exhibit 9010 -- Amanat Exhibit 9002, excuse  
14 me, 9010, 9013 and 9008.

15 You have a stack of documents with Amanat exhibit tabs in  
16 front of you?

17 A. Yes.

18 MS. GRISWOLD: Just to be clear for the record, your  
19 Honor, these are the unredacted versions of these exhibits that  
20 are dated -- and behind the unredacted, what I have handed up  
21 is the redacted version that came into evidence for each of  
22 these exhibits.

23 Q. Special Agent DeCapua, were you provided with each of these  
24 documents in preparation for your testimony today?

25 A. Yes.

Hc5Wtuz6

DeCapua - Direct

1 Q. And for each of them, did you then use the content to  
2 create a fabricated email to put into the Jon Smith account?

3 A. Yes, essentially it was copying and pasting.

4 Q. You testified before that you used the metadata provided by  
5 the defendant with regard to the May 8, 2009, email. Do you  
6 remember that testimony?

7 A. Yes.

8 Q. Were you provided metadata for all of these emails?

9 A. Not all of them. Only three of them.

10 Q. Were you provided metadata, for example, for the June 2,  
11 2011, email?

12 A. No, I wasn't.

13 THE COURT: Could you refer to it by exhibit number?

14 MS. GRISWOLD: Sure, your Honor. I apologize.

15 Q. For the 9013 -- the 9010 Amanat exhibit, which is dated  
16 June 2, 2011, were you provided any metadata or header  
17 information for this email?

18 A. No, I wasn't.

19 Q. Can you open it up on the screen, the one dated June 2,  
20 2011.

21 Even without the header information provided by the  
22 defendant, were you able to put this email into the Jon Smith  
23 account using the process that you showed the Court earlier?

24 A. Yes.

25 Q. How long did it take you to do that?

Hc5Wtuz6

DeCapua - Direct

1 A. 20 minutes.

2 Q. And can you click on the raw message just to show the  
3 metadata.

4 Now, to put these emails in the account, again, I just  
5 want to make sure I understand what it is that you used. Did  
6 you use anything beyond the software tools that you've shown  
7 and demonstrated to the Court today?

8 A. No.

9 Q. Now, the Jane Smith account now has that altered email that  
10 you put back in it, correct?

11 A. Correct.

12 Q. If you were to get a search warrant on that account right  
13 now, what would you expect to see?

14 A. I would get the altered email, the one that's on Yahoo  
15 server.

16 Q. The one that you changed to November 15, 2017?

17 A. Correct.

18 Q. Are you familiar with what is known as a 2703(d) order for  
19 header information?

20 A. I am.

21 Q. If you were to obtain a 2703(d) order for header  
22 information for the Jane Smith account, what would you expect  
23 to receive?

24 A. I would expect to receive the header information for the  
25 emails that exist on Yahoo's server at this time, which would

Hc5Wtuz6

DeCapua - Direct

1 be the spoof email.

2 Q. Had you seen this before, Special Agent DeCapua, in one of  
3 your cases, and by this, I mean an email altered and put back  
4 into a web mail account?

5 A. No.

6 Q. When you were asked to look into it, what was your process  
7 for determining if it could be done?

8 A. I researched by doing some Google searches and found some  
9 articles talking about how to upload emails into Yahoo Mail.

10 MS. GRISWOLD: May I approach, your Honor?

11 THE COURT: Yes.

12 Q. I have handed you what is marked for identification as  
13 Government Exhibits 3559 and 3560. Do you see those?

14 A. I do.

15 Q. Are these two of the articles that you found when you did  
16 some Google searching?

17 A. Yes.

18 Q. Can you read for the record the title of the first article?

19 A. The first article is titled "Is It Possible to Import  
20 Messages to Yahoo Mail?"

21 Q. That's 3559?

22 A. Yes.

23 Q. Can you read the title of 3560?

24 A. "Using Message ID Headers to Determine if an Email Has Been  
25 Forged."

Hc5Wtuz6

DeCapua - Direct

1 Q. So after reviewing Government Exhibit 2908, the email  
2 between Omar Amanat regarding pulling emails down to the  
3 Outlook account, you searched for these articles?

4 A. Yes.

5 Q. These articles, did you have to do anything beyond what  
6 these articles say? Did they tell you all of the steps?

7 A. They didn't tell me all the steps, no.

8 Q. What did you do to determine the rest of the steps?

9 A. I just -- I knew my -- I had a basic understanding of how  
10 inbox files work and that they're saved as text documents on  
11 the computer. I had an understanding of the difference between  
12 an email header and email content, and I experimented and  
13 eventually came up with a solution that worked.

14 Q. Prior to two weeks ago, did you have any involvement in the  
15 case involving Omar Amanat and Kaleil Isaza Tuzman?

16 A. No.

17 Q. Do you know any of the underlying facts of this case?

18 A. No.

19 MS. GRISWOLD: Unless the Court has further questions  
20 for this witness, I don't have any further questions.

21 THE COURT: All right. Cross-examination.

22 MR. JACKSON: Your Honor, may I ask for a five-minute  
23 recess.

24 THE COURT: Of course. We'll take a brief recess.

25 You may step down.

Hc5Wtuz6

DeCapua - Direct

1 MS. GRISWOLD: Your Honor, in light of Mr. Maiden  
2 leaving, I defer to how the Court wants to handle it. If we  
3 wanted to, we'd have to put him on now, prior to the cross. I  
4 don't know what Mr. Jackson wants to do. We can bring  
5 Mr. Maiden back tomorrow, but I think those are our options.

6 MR. JACKSON: I would be happy to have Mr. Maiden go  
7 before my cross, but if we could take our five-minute recess,  
8 that would be helpful.

9 THE COURT: All right. We can take a recess.

10 MS. GRISWOLD: I don't know if that's going to work,  
11 your Honor. I apologize. Special Agent Amato is going to put  
12 in some testimony and charts that I was then going to have  
13 Mr. Maiden, because I haven't had as much access to him, so I  
14 think we're going to have to have Mr. Maiden tomorrow, if  
15 that's OK with the Court.

16 THE COURT: That's fine with me. Frankly, I'd rather  
17 not break up this agent's examination anyway, so we'll just  
18 have to go through Maiden tomorrow.

19 All right. We'll take a few minutes.

20 MR. JACKSON: Thank you.

21 MS. GRISWOLD: I'm passing 3500 for Special Agent  
22 DeCapua to Mr. Jackson right now.

23 THE COURT: All right.

24 (Recess)

25 THE COURT: Please be seated.

Hc5Wtuz6

DeCapua - Cross

1 Mr. Jackson, please proceed.

2 MR. JACKSON: Thank you, your Honor.

3 CROSS-EXAMINATION

4 BY MR. JACKSON:

5 Q. Good evening, sir.

6 A. Good evening.

7 Q. If I could ask you to move the mike just a bit closer to  
8 you.

9 Now, Special Agent DeCapua, am I correct that you have  
10 been a special agent, you said since 2009?

11 A. That's correct.

12 Q. And how much time is it that you have been on the cyber  
13 squad again?

14 A. Since 2014, so a little over three years.

15 Q. And during the -- you described the SANS training and DEx  
16 training.

17 I'm sorry. Verbal answer.

18 A. Yes.

19 Q. How long did the SANS and DEx training take?

20 A. DEx training was two weeks on site. SANS training, I would  
21 self-study at home with the exception of one course. The one  
22 course I took on site was one week full time. The self-study  
23 would normally take me two or three months of self-study before  
24 I challenged the exam.

25 Q. All right. And over the course of the time that you have

Hc5Wtuz6

DeCapua - Cross

1 been working as a cyber agent, approximately how many weeks  
2 would you say you've spent in the type of technical training  
3 we're talking about?

4 A. Spent in technical training?

5 Q. Sure.

6 A. So, over the course of three years, it would be very hard  
7 to quantify, but --

8 Q. Just a rough estimate.

9 A. Three months.

10 Q. Some of that was at Quantico?

11 A. That's correct.

12 Q. Some of that has been sort of in the field, in the New York  
13 field office?

14 A. Yes.

15 Q. And you've been working with some of the best cyber agents  
16 in the world in terms of this training, right?

17 A. Yes.

18 Q. Now, to be very clear, in the two weeks that you've been  
19 looking at this issue, you have been working closely with Agent  
20 Amato, right?

21 A. Yes.

22 Q. And you've been consulting with the prosecutors?

23 A. Yes.

24 Q. And during that time, you have evaluated, you've spoken to  
25 other people about the possibility that you just demonstrated

Hc5Wtuz6

DeCapua - Cross

1 for us, right?

2 A. Yes.

3 Q. You talked to other cyber agents?

4 A. Yes.

5 Q. Have any of the other cyber agents ever seen done what you  
6 just described?

7 A. No.

8 Q. And you had never seen it done?

9 A. I have never seen it done, no.

10 Q. When was the first time that you realized that you had the  
11 capability to do what you just demonstrated?

12 A. I think it was late last week.

13 Q. Can you give us any guess as to about when?

14 A. I want to say Thursday or Friday, but I'm not 100 percent  
15 sure about that.

16 Q. And am I correct that since then, you haven't asked Yahoo  
17 to engage in any sort of analysis of the email accounts that  
18 you manipulated?

19 A. I have not, no.

20 Q. So you don't know whether or not there is any data that  
21 Yahoo has that showed that you uploaded an email to the account  
22 that had been manipulated?

23 A. Not that I know of.

24 Q. Right. I'm just saying you haven't asked that question of  
25 Yahoo, right?

Hc5Wtuz6

DeCapua - Cross

1 A. I have not asked that question, no.

2 Q. You don't have any technical data in that area?

3 A. There is no technical data in that area. That's correct.

4 Q. Right. You also demonstrated for us -- well, let me back  
5 up. I'm going to come back to that, but let me back up.

6 I want to take a look at what was marked as Government  
7 Exhibit 3555. And actually, before we get to that, just to be  
8 clear here, the method that you just demonstrated, you have not  
9 been able to find any technical data that supports that that  
10 happened in this case, right?

11 A. I'm a little confused by what you mean by that question.

12 Q. You described a number of things that you saw on some of  
13 these emails that you thought was suspicious, right?

14 A. That's correct.

15 Q. But you don't have any sort of forensic or technical data  
16 that says these emails were created by the method that you just  
17 described, the defense exhibit emails?

18 A. There wouldn't be any signs or traces.

19 Q. Right, so you don't have any signs or traces or anything to  
20 point to there?

21 A. Correct.

22 Q. So your theory as to how this could be done, you don't have  
23 any technical information to connect that to the actual  
24 exhibits, right?

25 THE COURT: I think what he's testified to is there

Hc5Wtuz6

DeCapua - Cross

1 wouldn't be any forensic or technical data showing the  
2 manipulation.

3 Right?

4 THE WITNESS: That's correct.

5 THE COURT: Is that what you said?

6 THE WITNESS: Yes.

7 MR. JACKSON: Let me explore that just a bit, Judge,  
8 because I think it raises a great question.

9 Q. You don't actually know whether there could be technical  
10 data that could be supported if there was manipulation, right?

11 A. I don't know about the logs that Yahoo may keep. I suspect  
12 they wouldn't log anything like this, but in terms of technical  
13 data, I'm assuming that you're referring to the header  
14 information that's on the emails.

15 Q. Right. Between the logs, whatever data Yahoo has, you  
16 don't know as you sit here today whether there would be  
17 information that would show what you just described occurred,  
18 right?

19 A. You're right. I don't know.

20 Q. At bottom, we have your theory here, and it's really a  
21 theory as to how someone could accomplish this, right?

22 A. Yes.

23 Q. OK. Now, turning to -- and by the way, any email in the  
24 world, under your theory, could be inauthentic, right?

25 A. That's true.

Hc5Wtuz6

DeCapua - Cross

1 Q. It's conceivable that someone could, with any email in the  
2 world, use these same tools to create essentially a fabricated  
3 email, right?

4 A. Yes.

5 Q. Now, in Government Exhibit 3553, I was a little -- I  
6 apologize, because I was a little slowly following your  
7 description in the creation of the document, but were you  
8 responsible for creating this?

9 A. Yes.

10 Q. OK. So you actually looked at each one of the accounts in  
11 question in order to develop this information?

12 MS. GRISWOLD: Objection. It's just one account.

13 THE COURT: I'm sorry. Are you asking about 35 --  
14 which exhibit are you asking about?

15 MR. JACKSON: I'm sorry. I'm asking about 3553-A,  
16 your Honor -- I'm sorry. 3555.

17 THE COURT: Yes, you were using the wrong exhibit  
18 number. You're asking about Government Exhibit 3555.

19 MR. JACKSON: Yes, Judge.

20 THE COURT: OK. Go right ahead.

21 BY MR. JACKSON:

22 Q. So there's one account that relates to this, right; it's  
23 kit@kitcapital.com?

24 A. That's correct.

25 Q. And it was actually you who looked at the search warrant

Hc5Wtuz6

DeCapua - Cross

1 returns from two weeks ago to match up each one of these emails  
2 that you found in the account, right?

3 A. Yes.

4 Q. But you didn't find in the account any original sent  
5 version of each one of these emails, did you?

6 A. So, I don't know.

7 Q. Well, let me try and explain what I mean here. Your  
8 theory, right, is that for all of these emails, you said  
9 presence of emails, right, and your theory is that for the  
10 authentic emails, we would expect to see the sent-out version  
11 in the kit@kitcapital.com account, right?

12 A. Yes.

13 Q. Not just the forward of it but the actual version that was  
14 leaving the kit@kitcapital.com account?

15 A. Yes, the original sent email.

16 Q. I'm correct, though, right, it's not the case that for all  
17 of these, the original sent-out version is in the  
18 kit@kitcapital.com account?

19 A. We did identify a lot of the original sent emails in the  
20 kit@kitcapital.com account.

21 Q. I understand a lot, but my question is just a little bit  
22 different, Special Agent. My question is, you didn't find all  
23 of them, did you?

24 A. I don't know if we found all of them.

25 THE COURT: Just so I'm clear, you've both been using

Hc5Wtuz6

DeCapua - Cross

1 the term "all of them." Are we talking about the eight emails  
2 that are listed on 3555? Is that what we're talking about, or  
3 are we talking about something more broadly?

4 MR. JACKSON: No. Precisely, Judge. We can start  
5 with that. I'm going to explore it a little bit more broadly  
6 after that, but right now what I started with was the eight  
7 exhibits that are on 3555, but I think Agent DeCapua was  
8 talking about something slightly broader.

9 THE COURT: Looking at the eight emails that are in  
10 Government Exhibit 3555, were you able to find the original  
11 sent version?

12 THE WITNESS: Yes, for the majority of them, if my  
13 memory is correct. And I'm not sure if we found every single  
14 sent version, but we did find some of them.

15 BY MR. JACKSON:

16 Q. Right, so you found some of them, but this document doesn't  
17 purport to indicate that you found all of them, right?

18 A. That's correct.

19 Q. And in fact, it is a fact, right, that, for example, email  
20 No. 5, the 5/8, 2009, at 10:21 p.m., that's just not in there,  
21 right, in the original sent version?

22 A. I don't know.

23 Q. You know if it was one of the emails that was identified in  
24 Special Agent Amato's declaration, right?

25 A. Yes.

Hc5Wtuz6

DeCapua - Cross

1 Q. You went through the declaration at the time that Special  
2 Agent Amato prepared it, right?

3 A. No.

4 Q. You assisted her in preparing it?

5 A. I did not.

6 Q. Have you read it now?

7 A. I haven't.

8 Q. OK, but you know it's referenced in there?

9 A. Yes.

10 Q. I gotcha. So my point being that you looked at this, as  
11 you sit here now, you're not aware of whether or not the 5/8,  
12 2009, at 10:21 p.m., in its original sent version was in those  
13 search warrant returns, right?

14 A. We found it in one of the threads at a very minimum, and I  
15 don't know if we found the original sent version in that email.

16 Q. Right, and just to be clear, finding it in the thread is  
17 very different from finding it in the original sent version?

18 Right?

19 A. Yes.

20 Q. In terms of the evidence you're now here with, right?

21 A. Yes.

22 Q. And that's because finding it in the thread means, by your  
23 theory, someone could have pasted that email in there and  
24 manipulated it, right? You read it?

25 A. Can you repeat that question?

Hc5Wtuz6

DeCapua - Cross

1 Q. Sure. Your testimony, right, is that when you only see it,  
2 and you only see the underlying, forwarded message, right, in  
3 the thread, it's impossible to determine its authenticity?

4 Right?

5 A. That's correct.

6 Q. Because that could be manipulated by anyone; you don't need  
7 to go through the procedure that you described, right?

8 A. That's correct.

9 Q. So what is the real jewel in terms of your analysis here is  
10 that the actual sent message is there, from your perspective,  
11 right?

12 A. Yes.

13 Q. And here, you're saying you weren't able to identify the  
14 original sent message for all of the emails that you know were  
15 sent or that you believe were sent by the kit@kitcapital.com  
16 account, right?

17 A. So, I don't know.

18 Q. All right. Let me ask you this. How much time did you  
19 spend going over the search warrant returns on the  
20 kit@kitcapital.com account?

21 A. About an hour.

22 Q. An hour. How did you do it?

23 A. So, I uploaded it into a local email client and I searched  
24 each email just manually. There was only like 40 of them or  
25 so. So I go through each one. I searched for key words. I

Hc5Wtuz6

DeCapua - Cross

1 looked at each one. I carved out the message ID as seen in the  
2 other exhibit that I created. I also searched for some key  
3 words using, using a search program, just to make sure I wasn't  
4 missing anything.

5 Q. Did you take a look to see if in your search warrant  
6 returns there are any indications that maybe Mr. -- first of  
7 all, let me withdraw that question.

8 You know that kit@kitcapital.com is for a person named  
9 Kaleil Isaza Tuzman? You have that level of familiarity with  
10 the case, right? You know who the defendants are, right?

11 A. So, I get the names confused, but that sounds right.

12 MR. JACKSON: OK. I think we can stipulate, the  
13 parties can stipulate we understand this is Mr. Isaza Tuzman's  
14 account.

15 Can I ask for that stipulation, Judge, from the  
16 government?

17 MS. GRISWOLD: Yes, your Honor.

18 THE COURT: Yes, go ahead.

19 BY MR. JACKSON:

20 Q. Did you take a look at all in the account in the search  
21 warrant returns to see if there were any indications in the  
22 search warrant returns that Mr. Isaza Tuzman's devices may have  
23 regularly deleted sent messages?

24 A. I don't think that type of information would be there, so  
25 no, I did not look for it.

Hc5Wtuz6

DeCapua - Cross

1 Q. You don't think it would be there? Well, let me show you  
2 something.

3 MR. JACKSON: Judge, I'm just going to apologize right  
4 now because I'm not going to have original hard copies of a lot  
5 of things. I did not know what I was going to be crossing on,  
6 but I have a copy to put on the Elmo, and I don't think there's  
7 any issue, because there's no jury.

8 Your Honor, at this point we would just briefly ask,  
9 temporarily ask if the Court would be willing to sequester  
10 Agent Amato for the remainder of this cross at issue.

11 THE COURT: Any objection from the government?

12 MS. GRISWOLD: No, your Honor. We can ask her to step  
13 out.

14 THE COURT: All right. Please.

15 MR. JACKSON: Thank you.

16 Q. OK. I want to show you a document which we'll mark as  
17 Amanat Hearing Exhibit 18.

18 THE COURT: There seems to be some light object at the  
19 top. What is that?

20 MR. JACKSON: We have a little bit of glare, Judge.

21 THE COURT: Is that a glare or something else?

22 MR. JACKSON: It's a little bit of glare.

23 Q. Can you see this, sir?

24 A. Yes.

25 Q. OK. So this is an email that I would proffer came from the

Hc5Wtuz6

DeCapua - Cross

1 search warrant returns, and we can confirm that later, but this  
2 is an email --

3 MR. JACKSON: I'm going to offer on that proffer  
4 Amanat Exhibit 18.

5 THE COURT: I can't hear you.

6 MR. JACKSON: I'm sorry. Let me speak up, Judge. I'm  
7 sorry. I'm going to offer on that proffer Amanat Exhibit 18.

8 THE COURT: Any objection?

9 MS. GRISWOLD: No, not on that basis.

10 THE COURT: OK. Then Amanat Exhibit 18 is received.

11 (Defendant's Exhibit Amanat 18 received in evidence)

12 BY MR. JACKSON:

13 Q. We have this email from Kaleil Isaza Tuzman. Can you see  
14 the date that this was sent, sir?

15 A. Yes.

16 Q. OK. What is the date?

17 A. It's May 9, 2009.

18 Q. And can you see who he's emailing?

19 A. It is to G. Scott Paterson.

20 Q. Can you read what it says in the actual email there?

21 A. "That's why I was emailing you. My Blackberry wiped my  
22 past emails more than a week old."

23 Q. Then there's like a sad face, right?

24 A. Right.

25 Q. And then what does it say after that?

Hc5Wtuz6

DeCapua - Cross

1 A. "Can you search under my name and see last email I sent you  
2 and I'll tell you if it was most recent? It covered a bunch of  
3 items."

4 Q. By the way, you don't know who G. Scott Paterson is, right?

5 A. No.

6 Q. And you see G. Scott Paterson responds to Mr. Isaza Tuzman,  
7 right?

8 A. Yes.

9 Q. And what does he say?

10 A. "My bberry dumps everything after 48 hours. Huge problem  
11 for me. I will search on computer when home. I did receive a  
12 laundry list email, and I responded to it, but I don't have  
13 either, unfortunately, on my bberry. Scott."

14 Q. Special Agent DeCapua, you've been involved in a lot of  
15 investigations involving devices, smartphones, etc.?

16 A. Yes.

17 Q. You are aware that depending on the settings on a device  
18 like that, deletion on the Blackberry device may also trigger  
19 deletion on the home client, right?

20 A. Yes.

21 Q. And so if something is deleted on a Blackberry device,  
22 sometimes it's gone forever, right?

23 A. Yes.

24 Q. And just to be clear, that's not an email you reviewed  
25 before you did any of your analysis in this case, right?

Hc5Wtuz6

DeCapua - Cross

1 A. So, I don't remember. I don't think so.

2 Q. You don't remember actually seeing that?

3 A. No.

4 Q. And it's not one that anyone discussed with you at the FBI?

5 A. No.

6 Q. But the fact that there is an email in the account  
7 indicating that on the precise date in question Mr. Isaza  
8 Tuzman is indicating that his Blackberry was deleting messages,  
9 it's a relevant factor in the type of analysis that you're  
10 doing here, right?

11 A. I would say yes. I'd want to see the email, the -- to  
12 verify that was in the account.

13 THE COURT: I'm sorry. You'd want to see what?

14 THE WITNESS: To see actual KITCapital emails to  
15 verify that that email that he just showed me was in the  
16 account, because I don't know. I don't remember seeing that  
17 email in our search warrant return.

18 MR. JACKSON: OK. I mean, we can deal with it later,  
19 but I'd be happy, if you want, to allow you to take a moment to  
20 take a look.

21 THE COURT: The government has looked at the emails,  
22 correct?

23 Did you look at the emails?

24 MS. GRISWOLD: We have the emails. I don't know. I  
25 can't proffer one way or the other. I take Mr. Jackson's

Hc5Wtuz6

DeCapua - Cross

1 proffer that they're in the email account.

2 THE COURT: OK.

3 MS. GRISWOLD: With that in mind.

4 THE COURT: OK.

5 BY MR. JACKSON:

6 Q. Now, I just want to go back to some of your earlier  
7 testimony about the things that you said stuck out to you when  
8 you first took a look at the 5:21 email from Mr. Isaza Tuzman.  
9 One of the things that you said in your testimony, right, is  
10 that if you see an email in two different accounts, that's  
11 significant evidence that an email is more likely to be  
12 authentic, right?

13 A. Yes.

14 Q. And in this case, you're aware that the government made its  
15 initial challenge to that email when it was under the belief  
16 that it only existed in one account, right?

17 A. Yes.

18 Q. And then you know now that subsequent to the initial  
19 challenge, the government discovered that the outbound email  
20 existed in another account, a second account, right?

21 MS. GRISWOLD: Objection.

22 THE COURT: We need to be very clear, very, very  
23 clear. You can't say "that email." Are you talking about the  
24 5:21 p.m. email? Is that the one you're talking about, or are  
25 you talking about all of Government Exhibit 3553? I just don't

Hc5Wtuz6

DeCapua - Cross

1 know what you're talking about.

2 MR. JACKSON: Let me be much more specific, your  
3 Honor. I apologize.

4 Q. The 5:21 email on May 8, 2009, has been the primary email  
5 that the FBI has focused its analysis on, right?

6 A. That's correct.

7 Q. That's the email that started the discussion, right?

8 A. Yes.

9 Q. And at the time that the FBI started looking at this issue  
10 with the prosecution, it was under the belief that the 5:21  
11 email only existed as a forward into the Sharif Amanat email  
12 account, right?

13 A. Yeah, it was part of a thread to a different email. We  
14 just saw it in the contents of the email.

15 Q. Right. And so the initial theory at that time of the FBI  
16 was that Mr. Amanat had simply typed the email, right, and  
17 forwarded it to his dad? Correct?

18 A. I wouldn't say it was the theory. I mean, I found some  
19 things that looked strange, and I pointed them out to the trial  
20 team when they asked me.

21 Q. OK, but you're aware that subsequent to the challenge being  
22 made to the authenticity of the Sharif Amanat email on May 8,  
23 2009, that included as a forward --

24 THE COURT: Sorry to interrupt, but you keep on  
25 talking about the Sharif Amanat email. I don't know what

Hc5Wtuz6

DeCapua - Cross

1 you're talking about. There's no Sharif Amanat on the email,  
2 as far as I -- maybe there is, at the top.

3 MR. JACKSON: I apologize, Judge.

4 THE COURT: But I don't think you've elicited who  
5 Sharif Amanat even is. Anyway, I'm just telling you I don't  
6 understand. I don't understand the examination.

7 MR. JACKSON: I completely get it, Judge. It's a  
8 little confusing. Let me try to short circuit this.

9 Q. I'm returning to Government Exhibit 3553, and what you can  
10 see is this is a -- this is what you understand was the defense  
11 exhibit that was provided to the government, right?

12 A. Yes.

13 Q. And it's been made a government exhibit for this hearing,  
14 right?

15 A. Yes.

16 Q. And what it is, is we have on May 8, 2009, down at the  
17 bottom, the email from Mr. Isaza Tuzman to four people, right?

18 A. Yes.

19 THE COURT: I'm sorry. Where are you?

20 MR. JACKSON: I'm at the bottom of the page, your  
21 Honor.

22 THE COURT: The bottom of the first page?

23 MR. JACKSON: Yes, your Honor, the bottom of the first  
24 page.

25 THE COURT: OK.

Hc5Wtuz6

DeCapua - Cross

1 MR. JACKSON: There's an email from Kaleil Isaza  
2 Tuzman.

3 THE COURT: At 5:21.

4 MR. JACKSON: At 5:21.

5 Q. There are things that are forwarded above, but this is the  
6 primary focus from the standpoint of your analysis, right?

7 A. Yes.

8 Q. And what this document is, is a forward?

9 THE COURT: Are you saying what this email is?

10 MR. JACKSON: I'm saying what Government Exhibit 3553  
11 is, is a forward of the 5:21 email, right, that is a forward  
12 to -- you see beneath this --

13 THE COURT: I think if you want to go down this road,  
14 you're welcome to walk through the emails with the agent. That  
15 might help.

16 MR. JACKSON: That might help.

17 THE COURT: Yes, that might be helpful.

18 BY MR. JACKSON:

19 Q. OK. What is the next thing that you see after the 5:21  
20 email, sir? What's the next thing temporally that happens in  
21 this chain?

22 A. Looks like a forward and reply with the same subject line  
23 as the previous email, and it's from Omar to someone named  
24 Afzal Amanat.

25 Q. And above that, you see there's a response from an email

1 Hc5Wtuz6

2 DeCapua - Cross

3 address chach786@aol.com to omar@amanatcapital.com and  
4 sharifamanat@yahoo.com?

5 A. That's right.

6 (Continued on next page)

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

HC5TTUZ7

DeCapua - Cross

1 BY MR. JACKSON:

2 Q. So the point being when you began your analysis, you --

3 THE COURT: Before we leave that, I want to make sure  
4 understand what the top email is.

5 So the Chach email at the top, that's a reply to the  
6 forward?

7 MR. JACKSON: Yes, your Honor.

8 THE COURT: I'm asking the witness.

9 The Chach email is a reply to Omar's email at 5:27?

10 THE WITNESS: It looks like it's a forward of the  
11 forward.

12 THE COURT: That's why I'm confused. That's why I'm  
13 confused.

14 I'm also confused because the top email has  
15 different -- well, it includes this Sharif name for the first  
16 time, and so I just -- so you know, I don't understand the  
17 sequence here.

18 MR. JACKSON: Absolutely, Judge, and let me give a  
19 brief proffer of what the sequence is, and the agent can  
20 perhaps confirm if that's his understanding. I know he doesn't  
21 know these people, but Chach is the email address of  
22 Mr. Amanat's uncle, and that's Afzal, known as Chach.

23 THE COURT: So the Afzal Amanat in the 5:27 email,  
24 that's the Chach person at the top, right?

HC5TTUZ7

DeCapua - Cross

1 MR. JACKSON: Exactly, Judge. And Sharif Amanat is  
2 Mr. Amanat's father.

3 THE COURT: Okay.

4 BY MR. JACKSON:

5 Q. And by the way, Special Agent Decapua, it's not uncommon to  
6 see in a forward or a reply just a name as opposed to the email  
7 address itself, right?

8 A. That's correct.

9 Q. And sometimes you will see the email address, right?

10 A. Yes.

11 Q. There are a lot of different factors that could impact what  
12 is actually shown in terms of an email address versus just a  
13 name, right?

14 A. That's correct.

15 THE COURT: Well, let me ask you this, so the 5:27  
16 email is a forward from Omar to his uncle Afzal, that much I  
17 understand. What's the Chach email?

18 MR. JACKSON: Chach is the email address for Afzal.

19 THE COURT: I understand that, I'm asking the agent  
20 his understanding of what that email is.

21 Do you understand what I mean?

22 THE WITNESS: So based on what counsel just told me --

23 THE COURT: No, I don't want you to rely on what  
24 counsel told you. You can rely on who the people are, that  
25 Afzal was the uncle, Chach is the uncle, Sharif is the father,

HC5TTUZ7

DeCapua - Cross

1 that's fine, but from looking at the document, can you tell how  
2 the Chach email, the top email, relates to the 5:27 email?

3 THE WITNESS: No.

4 THE COURT: No.

5 THE WITNESS: On the face of the document I can't  
6 tell.

7 THE COURT: So you don't know whether it's a reply or  
8 something else, you just don't know.

9 THE WITNESS: Going to the subject line, it says it's  
10 a forward.

11 THE COURT: And you mean just because it has the  
12 double FWD, FWD?

13 THE WITNESS: Yes.

14 THE COURT: I'm having trouble understanding -- so are  
15 you saying then -- well, who forwarded the -- can you tell who  
16 forwarded the 5:27 email?

17 I understand you say it's a forward, but can you tell  
18 who forwarded it to who?

19 THE WITNESS: It looks like omar@amanatcapital  
20 forwarded it to Afzal Amanat. That's the forward.

21 THE COURT: That's the 5:27.

22 THE WITNESS: That's the 5:27. And if Chach 786 is  
23 Afzal Amanat, then it would make sense for the next forward to  
24 be from chach786@aol.com and forwarding it to Omar and Sharif,  
25 but there's nothing on the face of the document that indicates

HC5TTUZ7

DeCapua - Cross

1 that Afzal is chach786@aol.com.

2 THE COURT: But that's counsel's representation.

3 MR. JACKSON: Yes.

4 Q. And this brings up sort of an important point I was going  
5 to and explore later, but I think it is important.

6 Let me ask you, what is autofill, Special Agent  
7 DeCapua?

8 A. What did you say?

9 Q. What is autofill in the context of sending emails on a web  
10 client? Do you know what that is?

11 A. Autofill? I don't know what that is.

12 Q. Let me try to walk you through it. When you forward an  
13 email on a web client, you can forward it to other people,  
14 right?

15 A. Right.

16 Q. And if you start to type a name, if the email web client is  
17 familiar with the name, it may bring up multiple email  
18 addresses that are connected to that name, right?

19 A. Right.

20 Q. And it will give you the option of clicking on one or the  
21 other in some email clients, right?

22 A. That's correct.

23 Q. So in your experience, it's not uncommon for emails sent  
24 between people who are familiar with more than one email  
25 address to sometimes send to one address and sometimes send to

HC5TTUZ7

DeCapua - Cross

1 another address?

2 A. I mean I don't think that's true.

3 Q. Sorry, you're telling me you don't think it's true that in  
4 your investigations you haven't seen, for example, situations  
5 where in a corporation a person sometimes sends to the personal  
6 address, personal like gmail address of an individual, and also  
7 sometimes sends to their business address, like their IBM  
8 account?

9 MS. GRISWOLD: Your Honor, I object. The original  
10 question is is it common, then is it sometimes. I just object  
11 as to form.

12 MR. JACKSON: I said it's not uncommon.

13 THE COURT: Sustained.

14 Q. Well, you have seen that, right?

15 A. Yes.

16 Q. And it's not something that is uncommon in your  
17 observation, right?

18 THE COURT: So I understand, you're asking him it's  
19 not uncommon for somebody to email another person at different  
20 email addresses, is that what you're saying?

21 MR. JACKSON: Yes, your Honor.

22 THE COURT: If they were sending to multiple email  
23 addresses, is it true they may sometimes send to one email  
24 address and on occasion send to a different one?

25 THE WITNESS: The only thing I could speak about is

HC5TTUZ7

DeCapua - Cross

1 personal experience of messing up. I don't know what the other  
2 intentions of people sending emails is. I never ran across  
3 anything in any of my cases where that has been an issue or  
4 ever been raised. Me personally, I have on rare occasions sent  
5 it to a wrong email address when I meant to send it to a  
6 different one, but it was the same person who controlled both.

7 Q. Putting aside accidents, you have friends with multiple  
8 email addresses, right?

9 A. Yes.

10 Q. And you sometimes send to one email address or the other,  
11 right?

12 A. No.

13 Q. You always send to the exact same email address?

14 A. Yes.

15 Q. Okay.

16 THE COURT: Why is that?

17 THE WITNESS: Usually people only check one.

18 THE COURT: Okay.

19 Q. Are there any FBI agents -- well, this is not a good  
20 example because the FBI's email system is a closed system,  
21 right?

22 A. We have an external email system as well.

23 Q. You have a Blackberry as an FBI agent?

24 A. I have an Android.

25 Q. On your Android you have both the personal email addresses

HC5TTUZ7

DeCapua - Cross

1 of some of your fellow agents as well as the FBI addresses for  
2 your fellow agents, right?

3 A. Not on my work phone, just the professional email  
4 addresses.

5 Q. I see. Anyway, the point being this is the first email  
6 that you had that triggered your beginning of this  
7 investigation in this analysis on your part, right?

8 A. That's correct.

9 Q. And at the time that you got it, you did not know whether  
10 it was possible to access the Omar Amanat email address that is  
11 listed right there, right?

12 A. For the government to access it?

13 Q. Right.

14 A. I assumed it would need a search warrant.

15 Q. What I'm saying is you weren't aware of whether or not the  
16 email, the 5:21 email that we see here from Kaleil Isaza Tuzman  
17 at the bottom of the chain, you weren't aware that existed in  
18 any other place, right?

19 A. That's correct.

20 Q. And what you learned subsequently is that the defense had  
21 notified the government that they had access to the Omar Amanat  
22 account and that on the Omar Amanat account you could see the  
23 inbound message from Kaleil Isaza Tuzman, right?

24 A. Yes.

25 Q. Now the second thing that you noticed that you said gave

HC5TTUZ7

DeCapua - Cross

1 you trouble is that there were both EDT time and EST times on  
2 there?

3 A. That's right.

4 Q. And so it's -- the Kaleil Isaza Tuzman email at 5:21 is in  
5 EDT time, right?

6 A. Yes.

7 Q. And then right here in the middle email it's from Omar  
8 Amanat to Afzal Amanat, it's in Eastern Standard Time, right?

9 A. Yes.

10 Q. And the top, the 7:32:41 is on EDT, right?

11 A. That's correct.

12 Q. It's not your testimony that the mere fact that an email  
13 chain shows both EDT and EST is conclusive evidence of some  
14 sort of fabrication, right?

15 A. Not conclusive evidence, no.

16 Q. In fact, it's entirely possible for an authentic email  
17 chain to have both EDT and EST on it, right?

18 A. So I don't know that for sure.

19 Q. Right. So this was a suspicion that you had, but you don't  
20 actually know whether or not that is a technological issue,  
21 right?

22 A. I don't know.

23 Q. But to be clear, nothing in your training that you can  
24 point us to confirms that there is some issue with an email  
25 chain having EDT and EST in there, right?

HC5TTUZ7

DeCapua - Cross

1 A. I would expect it to be consistent.

2 Q. Right.

3 A. Just because if it was Mountain Time and EST, then yeah,  
4 that's normal. But for it to be the same time zone but one on  
5 daylight and one not, I expect it to be consistent.

6 Q. But to focus in on my question, you can't point us to  
7 anything that you learned in your training that says that where  
8 you see EDT or EST in the same chain that that is some  
9 indication of fabrication, right?

10 A. In my training I'm taught to look for inconsistencies.  
11 It's nothing conclusive, but it is an inconsistency.

12 Q. What I'm saying is you don't know whether there is any  
13 technological real oddity about it, right?

14 MS. GRISWOLD: Objection.

15 THE COURT: I don't understand the question.

16 Q. I think what I'm saying is you noted it as an  
17 inconsistency, but there's nothing that you can point us to  
18 that says this isn't something that happens in non-fabricated  
19 emails, right?

20 A. I don't know.

21 Q. Okay. Now --

22 THE COURT: I want to make sure I understand. I  
23 obviously understand what Eastern Standard Time is. Do you  
24 understand what Eastern Daylight Time is?

25 THE WITNESS: Yes.

HC5TTUZ7

DeCapua - Cross

1 THE COURT: How do the two relate to each other? Is  
2 that some reference to Daylight Savings Time, is that what  
3 Eastern Daylight Time is?

4 THE WITNESS: So my understanding is there used to be  
5 places in the United States that were on the Eastern time zone  
6 that did not recognize the Eastern Daylight time zone, places  
7 in Indiana, I think, for one example. So you had to  
8 differentiate depending on time of year whether you were  
9 talking about Eastern Standard Time or Eastern Daylight Time.  
10 Frankly, EDT, I don't see very often at all.

11 THE COURT: I don't either. Okay.

12 BY MR. JACKSON:

13 Q. Just to be clear also, one of the things -- one of the  
14 regular investigative challenges that you deal with is the fact  
15 that emails are often no longer in existence several years  
16 after they have been sent, right?

17 A. So they can be deleted, but I wouldn't say that they're  
18 often deleted. We find things that go back to early 2000s in  
19 some of our search warrants.

20 Q. But you are also aware, right, that many people delete some  
21 of their emails, right?

22 A. It's possible that people delete emails, yes.

23 Q. And in a lot of companies there are regular deletion of  
24 emails, right?

25 A. Not that I'm familiar with. It's possible, absolutely.

HC5TTUZ7

DeCapua - Cross

1 Q. You're not familiar with any companies that have policies  
2 that they regularly expunge emails? That's not something that  
3 you come across?

4 A. I can speak to the FBI's policy, and we keep everything.

5 Q. But you interface with companies in your role as a cyber  
6 agent, right?

7 A. Yes.

8 Q. And you have dealt with companies that have told you we  
9 purge emails after X amount of time?

10 A. I never have.

11 Q. You never dealt with that?

12 A. Never.

13 Q. Okay. But whatever the case may be, it is your experience,  
14 right, that sometimes witnesses would describe communications  
15 to you that they remember that are no longer accessible, right?

16 A. I can't think of one off the top of my head, but yeah,  
17 that's possible.

18 Q. Okay. Now are you aware that the omar@amanatcapital  
19 account, amanatcapital.com account, just to be very clear, you  
20 know that's a Yahoo account, right?

21 A. So I'm not sure about that. I have a chart that would  
22 refresh my memory.

23 MR. JACKSON: I would be happy to have the Special  
24 Agent DeCapua look at anything that might help him refresh his  
25 recollection.

HC5TTUZ7

DeCapua - Cross

1 Q. If you could tell us what it is, I would be happy for the  
2 government to produce it.

3 MS. GRISWOLD: Which chart?

4 THE WITNESS: The chart that explains whether or not  
5 the email was found.

6 MS. GRISWOLD: The full chart?

7 THE WITNESS: The full chart.

8 MS. GRISWOLD: That is 3555A.

9 May I bring it up to the witness to see if this is the  
10 chart?

11 THE COURT: Sure.

12 THE WITNESS: So I thought this email was part of this  
13 chart, but it's not, so I don't know if it is a Yahoo account  
14 or not.

15 Q. So you weren't asked to look into whether or not this was a  
16 Yahoo account or anything like that?

17 A. I don't remember.

18 Q. Okay. And you have no knowledge as to whether or not this  
19 account is linked to another account that Mr. Amanat had on  
20 Yahoo?

21 A. I have no idea.

22 Q. Are you familiar with a feature that Yahoo had called the  
23 catch all mailbox?

24 A. No.

25 Q. Are you familiar with the fact that Yahoo allows people to

HC5TTUZ7

DeCapua - Cross

1 purchase a domain name for their business, like  
2 omar@amanatcapital.com and have it actually be hosted by Yahoo?

3 A. I know that some web mail services do offer that, and it's  
4 quite common. I don't know if Yahoo did in 2009.

5 Q. But it's something that you're familiar with that web mail  
6 services offer?

7 A. Yes.

8 Q. And you're also aware that where a person has multiple web  
9 mail addresses, sometimes they could have linked accounts,  
10 right?

11 A. Yes.

12 Well, when you say "linked accounts," could you be  
13 more specific?

14 Q. Well, they could sometimes have one account that allows  
15 them to send from two different aliases, right, two different  
16 email addresses?

17 A. So I know you can do that from a local mail app, you can  
18 sync it with as many accounts as you want, and you can pick  
19 which address you want things to be send from.

20 Q. Right. And you also know that Yahoo allows people to save  
21 information to specific folders within the Yahoo account  
22 associated with a particular email address, right?

23 A. Yes, that's correct.

24 Q. And they can move things between folders within the Yahoo  
25 account?

HC5TTUZ7

DeCapua - Cross

1 A. Yes.

2 Q. Okay. Now I want to show you something marked -- let me  
3 back off of that.

4 Now I'm correct then November 17 was when you were  
5 first taking a look at this, right, at the email that we have  
6 been talking about, the 5:21 email?

7 A. That sounds about right.

8 Q. Let me show you something, and I want to ask you if it  
9 refreshes your recollection, which is marked as 3539-02.

10 A. Yes, that date is correct.

11 Q. And just to be clear, on that day when you said after --  
12 what happened is the prosecutors forwarded you the email that  
13 we have been talking about, right, from the Sharif account?

14 A. That's correct.

15 Q. And what your response to AUSA Griswold was is that you  
16 thought the only way you could think of verifying the chain's  
17 authenticity was to search the server records of  
18 kitcapital.com, right, Amanat Capital and KCP Capital for each  
19 intermediary email and chain?

20 A. Yes.

21 Q. And you said you do find it very suspicious that the  
22 formatting of the email changes in the middle of the chain,  
23 right?

24 A. That's right.

25 Q. You said I'm sorry I can't be of more help?

HC5TTUZ7

DeCapua - Cross

1 A. Correct.

2 Q. And to be clear, formatting of an email changing within a  
3 chain, while you may find it suspicious, is not actually  
4 evidence of fabrication, right?

5 MS. GRISWOLD: Objection.

6 THE COURT: Grounds?

7 MS. GRISWOLD: The term "evidence." I guess he can  
8 answer. I'll withdraw the objection.

9 A. It's an inconsistency.

10 Q. It's another inconsistency. And you told us that you were  
11 trained to focus on inconsistencies, right?

12 A. That's correct.

13 Q. But certainly a person can change the formatting in the  
14 middle of an email chain, right?

15 A. Yes, but I think you have to manually intend to change the  
16 formatting in the middle of the email chain.

17 Q. But certainly it's the case that sometimes people will copy  
18 and paste an authentic email that they received and forward  
19 that along, right?

20 A. Yes.

21 Q. And whether they do that, or if they forwarded it directly,  
22 it could impact the way the formatting ultimately looks in the  
23 chain, right?

24 A. I think so.

25 Q. It's also the case that different types of software will

HC5TTUZ7

DeCapua - Cross

1 alter an email chain in different ways, right?

2 A. I don't know that.

3 Q. Well, you are aware that an email may look different if  
4 it's forwarded from a Blackberry than it might if it's  
5 forwarded from a desktop computer, right?

6 A. Perhaps, yes.

7 Q. It's also possible that certain types of web clients  
8 will -- when an email is forwarded from one type of web client  
9 it may look different from the way a different type of web  
10 client adjusts the email when it's forwarded, right?

11 A. I think so, yes, but I haven't experimented with it so I  
12 can't definitively say yes, but --

13 Q. You're not an expert in all of the machinations of email  
14 web clients, right?

15 A. Of how emails were forwarded and replied and any changes.

16 Q. Right. But the fact of the matter is you're generally  
17 aware that all of the things that I just listed are things that  
18 could impact the way a chain of emails looks, right?

19 A. That's correct.

20 Q. Now did the government discuss any of the emails that are  
21 in discovery, the government's discovery in this case, with you  
22 and ask you to compare those to the analysis that you were  
23 doing with what you were seeing in the search warrant returns?

24 THE COURT: I don't understand the question.

25 MR. JACKSON: Let me try to clear that up, Judge, I'm

HC5TTUZ7

DeCapua - Cross

1 sorry.

2 Q. You're aware there are a number of emails that the  
3 government has in its investigation that it believes are  
4 authentic, right?

5 A. Correct.

6 Q. And those emails have been produced to defense in  
7 discovery, right?

8 A. Yes.

9 Q. And you're aware that those emails were retrieved from  
10 various sources, right?

11 A. Yes.

12 Q. Like some were retrieved from search warrants of different  
13 accounts?

14 A. Yes.

15 Q. Some were retrieved by subpoena, right?

16 A. Yes.

17 Q. And has the government asked you to compare the features  
18 that you found suspicious here in the 5:21 email with any of  
19 the features in the emails that it believes to be authentic?

20 A. So for the ones that were authored by kit@kitcapital, I did  
21 compare some of the features from the one that was suspicious  
22 to the ones that we found in the search warrant return that we  
23 know are likely authentic.

24 Q. Okay. And that comparison revealed that some of the things  
25 that you initially thought was suspicious were not quite as

HC5TTUZ7

DeCapua - Cross

1 suspicious as you originally thought, right?

2 A. No.

3 Q. Well, one of the things that you're aware Special Agent  
4 Amato identified as suspicious was the fact that for the same  
5 email from --

6 THE COURT: I'm confused. Now you're asking him about  
7 something that Agent Amato found suspicious as opposed to  
8 something that he found suspicious? I'm confused.

9 MR. JACKSON: Sorry, Judge, I think his testimony was  
10 that he had communicated with Agent Amato during his analysis.  
11 I don't mean to muddy the waters, but he looked at this  
12 email --

13 Let me ask him. I will focus right now on him.

14 Q. Do you believe that the fact that times for the same email  
15 showing up different in different emails is an indication -- is  
16 an inconsistency indicative of potential fabrication?

17 A. So without context, looking at an email thread and looking  
18 at the times changing, that is something that you want to focus  
19 on. You want to make sure that the timeline that the email  
20 thread purports is in the realm of possibilities.

21 Q. Okay. But --

22 THE COURT: I thought what your question was -- maybe  
23 I misunderstood your question. I thought you were suggesting  
24 the same email is a different time. Did I misunderstand?

25 MR. JACKSON: That's what I was asking, if he --

HC5TTUZ7

DeCapua - Cross

1 because I think there has been an indication that sometimes  
2 when you see an email in two different places and it has two  
3 different times, that's an inconsistency indicating potential  
4 fabrication, and I just want to know if this witness agreed  
5 with that conclusion or that statement.

6 THE COURT: So you have two different email accounts,  
7 the same email is in both, but it has different times?

8 MR. JACKSON: Right. Particularly -- yeah, exactly.

9 THE COURT: Would that be suspicious to you?

10 THE WITNESS: It depends. So when an email is sent  
11 from the sender it will have a specific time stamp, and then  
12 when it's received it will say the time stamp when it was  
13 received. And that could be off by seconds or a minute  
14 depending on network congestion. It's usually pretty fast  
15 though.

16 Q. And it could be off by much more than that depending on the  
17 clocks that are involved in different servers, right?

18 A. Yeah, of course.

19 Q. I want to show you two documents which are in discovery  
20 that are part of the chain, of the 5:21 email on May 8, 2009  
21 that we have been looking at, and these are documents that have  
22 Bates numbers USAO Tuzman 0 --

23 THE COURT: Can you just give him an exhibit number?

24 MR. JACKSON: Absolutely, Judge. We'll mark this as  
25 Amanat 16.

HC5TTUZ7

DeCapua - Cross

1 Q. And I'm going to take these one at a time because it's too  
2 hard to see, but you see here on the right side of Amanat  
3 Exhibit 16 you have a May 8 -- you have the May 8 email from  
4 Kamal Taraya, right?

5 A. Correct.

6 Q. And that's part of the chain of the original email that you  
7 were looking at, right?

8 A. I believe so.

9 Q. And the time here that this email was sent is reflected in  
10 the document on the right as what time?

11 A. It's Friday, May 8, 17:05:46, 2009.

12 Q. When you convert that out of military time, what time is  
13 that?

14 A. 5:05 p.m.

15 Q. Then in another email from discovery --

16 MR. JACKSON: Which I think we could stipulate, your  
17 Honor, there's no dispute that both of these are authentic  
18 emails.

19 MS. GRISWOLD: Your Honor, yes. I don't know which  
20 account we're being shown, but the content of what is on the  
21 screen we don't dispute is authentic.

22 THE COURT: All right.

23 Q. And so from the very same -- for the very same email,  
24 right, for Mr. Tayara, which is part of the chain in the 5:21  
25 email, there's a different time for sent, right?

HC5TTUZ7

DeCapua - Cross

1 A. Yes.

2 Q. How do you explain that?

3 A. Time zones most likely.

4 Q. Well, it's the same person who sent it, right?

5 A. Right.

6 Q. And so depending on who receives it, it may have different  
7 times reflected as the sent time, right?

8 A. Correct.

9 Q. So this is an example of an inconsistency that wouldn't  
10 actually be reflective of any fabrication, right?

11 A. Yes.

12 Q. The fact of the matter is we're dealing with very complex  
13 systems when we talk about email being sent around the world,  
14 right?

15 A. Yes.

16 Q. And while you are a very well trained agent, you don't  
17 purport to be a person who understands all the intricacies of  
18 the way those complex systems may impact the way an email  
19 looks, right?

20 A. Sure.

21 Q. Okay. Now another thing that you talked about during your  
22 original -- during your direct testimony is one of the things  
23 the FBI looked at was in regard to the 5:21 email, it searched  
24 for the Irfan Amanat account -- it searched an Irfan Amanat  
25 account in order to try to find receipt of the 5:21 email.

HC5TTUZ7

DeCapua - Cross

1 A. The gmail account.

2 Q. Right, the gmail account.

3 But you now know you searched the wrong account,  
4 right?

5 MS. GRISWOLD: Objection.

6 THE COURT: Grounds?

7 MS. GRISWOLD: He's not the one who searched the  
8 account. I thought Mr. Jackson didn't want us to rely on  
9 hearsay, so I don't think this is --

10 MR. JACKSON: I withdraw the question, your Honor. I  
11 didn't know.

12 THE COURT: All right.

13 Q. I want to take a quick look at Government Exhibit 3556.  
14 And this is the chart that you put together that we talked  
15 about on your direct examination, right?

16 A. Yes.

17 Q. The biggest point from when chart is the message ID is  
18 different from -- the highlighted yellow message -- than the  
19 other message IDs here, right?

20 A. That's correct.

21 Q. To be clear, though, all of the other messages that you  
22 obtained here besides the highlighted one you got from a  
23 different method, right?

24 A. Yes.

25 Q. So the highlighted yellow one is the one that you got from

HC5TTUZ7

DeCapua - Cross

1 the defense, right?

2 A. That's correct.

3 Q. And so where did you get all these other message IDs from?

4 A. It was from a search warrant return.

5 Q. On which account?

6 A. The kit@kitcapital.com.

7 Q. And you do know, right, that Mr. Isaza Tuzman utilized  
8 multiple devices to send emails, right?

9 MS. GRISWOLD: Objection, foundation.

10 MR. JACKSON: I'm asking if he knows.

11 THE COURT: Sustained.

12 Q. Do you know?

13 A. No.

14 Q. Okay. And the fact of the matter is if there was an issue  
15 where one of his devices regularly deleted emails, it would be  
16 much more likely that the emails that you would be able to find  
17 via the search warrant would have the message ID of the device  
18 that was not deleting emails, right?

19 A. Yes.

20 Q. And you agree with me, right, that the search warrant  
21 returns that you --

22 By the way, how many emails did you find in the search  
23 warrant returns?

24 A. I think there's about 40.

25 Q. It was a targeted search warrant, right?

HC5TTUZ7

DeCapua - Cross

1 A. Yes, three days.

2 Q. You didn't try to get the entire scope of Mr. Isaza  
3 Tuzman's email?

4 A. No.

5 Q. And you didn't engage in any analysis to try to determine  
6 whether or not -- what percentage of the emails that exist in  
7 discovery are now still available on Mr. Isaza Tuzman's  
8 kitcapital.com account, right?

9 A. Right.

10 Q. With these 40 emails or so that you received in this very  
11 targeted search, it's impossible for you to know whether or not  
12 you were able to capture the full range of message IDs that  
13 would have been associated with Mr. Isaza Tuzman's various  
14 devices, right?

15 A. That's correct.

16 Q. Okay. Did the government ask you to look into the issue of  
17 whether or not Mr. Maiden -- there was any evidence that  
18 Mr. Maiden deleted emails?

19 A. So I was provided the emails from that specific date range,  
20 but you're asking if I was to look into if he deleted them?

21 Q. Sorry, I may be confusing you because I don't -- I used a  
22 name I'm not sure you're familiar with. Do you know who Steve  
23 Maiden is?

24 A. I know he received the email that was in question.

25 Q. Right, he's one of the recipients of the email?

HC5TTUZ7

DeCapua - Cross

1 A. Right.

2 Q. But you don't have any independent knowledge of his  
3 investigatory significance with regard to case, right?

4 A. No.

5 Q. What I'm asking you is did the government ever ask you or  
6 anyone else from your unit that you're aware of to examine the  
7 question of whether there was evidence that Mr. Maiden deleted  
8 emails?

9 A. No.

10 Q. If it were true that Mr. Maiden regularly deleted emails,  
11 that would affect your analysis as to whether or not the fact  
12 that you didn't find the Maiden email is indicative of  
13 fabrication, right?

14 MS. GRISWOLD: Objection, find it where?

15 THE COURT: I can't hear you.

16 MS. GRISWOLD: The objection to where he's talking  
17 about when he said find the Maiden emails.

18 MR. JACKSON: Let me withdraw the question and let me  
19 rephrase, your Honor.

20 THE COURT: Please.

21 Q. You looked to Steve Maiden's hard drive, right, results to  
22 try to figure out if you could see this 5:21 email, right?

23 A. No, I was provided three days worth of emails from Steve  
24 Maiden's physical drives.

25 Q. Who provided them to you?

HC5TTUZ7

DeCapua - Cross

1 A. I think it was one of the paralegals.

2 Q. So you just had three days worth of Steve Maiden emails?

3 A. Yes.

4 Q. And the point of them providing those to you was for you to  
5 try to verify whether or not that batch of emails contained the  
6 5:21 email?

7 A. That's correct.

8 Q. And it wasn't in that batch of emails?

9 A. So I -- that wasn't my focus. I did do the work, but I am  
10 not 100 percent sure. I don't think it was.

11 Q. You're not sure. Okay. But let me ask you, are you aware  
12 of whether or not you or anyone in your squad was asked to  
13 examine the question of whether there was evidence that  
14 Mr. Maiden deleted emails?

15 A. No.

16 Q. Okay. Here's my point, the analysis that you have done --  
17 let me back up.

18 If Mr. Maiden did regularly delete emails, it would  
19 lower the likelihood that you would expect to see the received  
20 email in his emails, right?

21 A. It would lower the likelihood, but I know that there were  
22 emails for those days.

23 Q. But the fact that there were emails for those days does not  
24 mean that he couldn't have deleted specific emails, right?

25 A. Right.

HC5TTUZ7

DeCapua - Cross

1 Q. And you don't know anything about the facts of this case  
2 that would impact the question of whether or not he would have  
3 a motive or incentive to delete certain emails?

4 A. Correct.

5 Q. You haven't analyzed the rules on his computer to know  
6 whether or not there are specific -- whether there are things  
7 that have been deleted, right?

8 A. That's correct.

9 Q. Or whether there was regular deletion of certain types of  
10 emails. You don't know anything about that, right?

11 A. Correct.

12 Q. I want to ask you technical question. You're familiar with  
13 the relativity platform?

14 A. I'm familiar with what it is, and I have used it years ago,  
15 but I haven't used it recently.

16 Q. Can you explain to Judge Gardephe what the Relativity  
17 platform is?

18 A. I think it's an e-discovery tool that you can review emails  
19 in.

20 Q. You have used a lot of different e-discovery tools, right?

21 A. Relativity and Concordance are the two I used.

22 Q. It's something that you regularly use in your work, right?

23 A. No.

24 Q. Really, you don't use e-discovery tools at all?

25 A. Normally in reviewing emails I review them in the native

HC5TTUZ7

DeCapua - Cross

1 format and load them into a local mail client.

2 Q. Okay. Whatever the case may be, you are familiar with the  
3 fact that when a computer -- when a person deletes an email in  
4 Outlook, it goes into a deleted items folder, right?

5 A. That's correct.

6 Q. And over time, that email will ultimately be deleted,  
7 right?

8 A. I don't know for sure, I think it depends and how you  
9 configure Outlook.

10 Q. Right. There are some configurations where it will linger  
11 forever until the computer needs more space, right?

12 A. That's right.

13 Q. There are other configurations where it would be deleted  
14 after a certain amount of time, correct?

15 A. Correct.

16 Q. And there are some configurations where the amount of time  
17 before the email is put into the deleted folder are actually  
18 deleted is different than other configurations, right?

19 A. So I don't know for sure. That sounds right, though.

20 Q. It's your belief -- your best understanding is that there  
21 can be different amounts of time in different systems based on  
22 different settings for how long something will remain in the  
23 deleted folder, right?

24 A. That's correct.

25 Q. I want to show you something which is marked as Amanat

HC5TTUZ7

DeCapua - Cross

1 Exhibit 34. Actually, for the purpose of this hearing, I'm  
2 going to make this Hearing Exhibit 22. I believe it was marked  
3 as Amanat Exhibit 34 at trial.

4 Make this Hearing Exhibit 21. I would like you to  
5 look at Amanat Hearing Exhibit 21.

6 Can you see that, sir?

7 A. Yes, I can.

8 Q. And you see here that what's reflected are Stephen Maiden  
9 emails, right?

10 A. So I'm not familiar with this screen, but I see the name  
11 Steven Maiden emails in the upper left-hand corner, and the  
12 case name.

13 Q. Your knowledge of that is not important to the question I  
14 wanted to ask. Do you see where it says Stephen Maiden emails?

15 A. Yes.

16 Q. And you see there are folders under here that say original  
17 PSTs, QCE1, Archive PST, and calendar and deleted items?

18 A. Yes.

19 Q. That's typical of the way the architecture of a particular  
20 hard drive will be reflected on a discovery platform like this,  
21 right?

22 A. Yes.

23 Q. And so can you see here how many emails are reflected on  
24 this document as being in the deleted items folder for right  
25 here. Can you see that?

HC5TTUZ7

DeCapua - Cross

1 A. So I see ten in front of me.

2 Q. Sorry, let me focus you in.

3 You see that?

4 THE COURT: I don't understand what you're directing  
5 him to.

6 Q. Let me direct you to the number right here. Do you see  
7 where it says one of 25 of 395?

8 A. Yes.

9 Q. You understand that refers to the one to 25, the first 25  
10 of 395 items that would be in this bolded deleted items folder,  
11 right?

12 A. That's right.

13 Q. Now Outlook doesn't automatically move things without some  
14 sort of rule into a deleted items folder, right?

15 A. So my understanding is you can delete an email from  
16 Outlook, click it, and click delete, and it goes into deleted  
17 items folder. I don't know about setting rules to  
18 automatically delete things.

19 Q. But you described it, you can delete it and it can go into  
20 the deleted items folder, right?

21 A. Right.

22 Q. Now if a deleted items folder contained 395 documents, that  
23 would mean 395 documents were somehow placed into the deleted  
24 items folder at the time that the image was taken that is  
25 represented in this particular analysis, right?

HC5TTUZ7

DeCapua - Cross

1 A. Yes.

2 Q. And it would mean that they hadn't yet -- even if they're  
3 in a deleted items folder, they hadn't yet expired, right?

4 A. Yes.

5 Q. It's impossible to know after an email has been completely  
6 deleted from a computer whether or not it ever existed on the  
7 computer, right?

8 A. Well, it depends.

9 Q. Great point. It can be impossible to know, right?

10 A. It can be impossible, yes.

11 Q. Sometimes there is forensic evidence of the deletion even  
12 after it appears to be no longer accessible to a regular user,  
13 right?

14 A. That's correct.

15 Q. But in other situations, the deletion can be hard enough  
16 that the FBI looking at it would not be able to actually find  
17 those items anymore, right?

18 A. That's correct.

19 MR. JACKSON: I'm coming close to the end, Judge.

20 Q. On the computer that we looked at where you did your  
21 demonstration there is a folder called Plan B on it. Does that  
22 relate to this investigation?

23 A. It does.

24 Q. What is Plan B?

25 A. It is two videos I created today of me doing the

HC5TTUZ7

DeCapua - Redirect

1 demonstration.

2 Q. Just in case you couldn't get online access?

3 A. Yes.

4 THE COURT: We'll have to get to the bottom of that.

5 MR. JACKSON: I know, Judge.

6 Q. Just to be very clear, you can't state today with any  
7 reasonable degree of certainty that any of the emails that you  
8 looked at are in fact fabricated, right?

9 A. That's correct.

10 MR. JACKSON: No further questions of this witness at  
11 this time, your Honor.

12 THE COURT: Okay. Redirect?

13 MS. GRISWOLD: Very briefly, your Honor.

14 REDIRECT EXAMINATION

15 BY MS. GRISWOLD:

16 MS. GRISWOLD: First of all, your Honor, I would like  
17 to offer hard copies with government exhibit tabs of the emails  
18 that were contained in the Smith John email account that I  
19 examined Special Agent DeCapua during his direct. I could pass  
20 a copy up to the Court and the witness to confirm that that's  
21 what these are.

22 THE COURT: Okay.

23 Q. You testified on cross-examination that when you delete an  
24 email from the inbox it could go into the deleted emails  
25 folder, right?

HC5TTUZ7

DeCapua - Redirect

1 A. That's correct.

2 Q. And it is still on the computer?

3 A. Yes.

4 Q. And that's what we saw on the screen shot for Mr. Maiden's  
5 computer, correct?

6 A. Yes.

7 Q. You were also shown Amanat Exhibit 18 on the ELMO. That  
8 was the May 8, 2009 email between Mr. Isaza Tuzman and another  
9 individual that made reference to emails being deleted from a  
10 Blackberry. Do you remember those questions?

11 A. Yes.

12 Q. If an email account -- emails are deleted from a  
13 Blackberry, they can still exist on that individual's computer,  
14 correct?

15 A. That's correct.

16 Q. And if they're deleted from a Blackberry, they can still  
17 exist on the actual account within whatever platform or web  
18 mail service they're using to host that account, correct?

19 A. Yes.

20 Q. In that email that we just discussed, which is Amanat  
21 Exhibit 18, that made reference to Mr. Tuzman's use of a  
22 Blackberry. The metadata, the header information that you  
23 found for the 5:21 p.m. email provided by the defendant, what  
24 type of email device was that message ID affiliated with?

25 A. Apple mail.

HC5TTUZ7

DeCapua - Redirect

1 MS. GRISWOLD: May I, your Honor?

2 THE COURT: Yes.

3 Q. I have passed up what is marked for identification as  
4 3570A, 3570B, 3570C, 3570D and 3570E. Do you see those?

5 A. Yes.

6 Q. And for the record, 3570A appears to be an email dated  
7 Tuesday December 2nd, 2008?

8 A. That's correct.

9 Q. 3570B appears to be an email dated Thursday, June 2nd,  
10 2011?

11 A. Yes.

12 Q. 3570C appears to be an email dated Monday, March 26, 2012  
13 at 11:34 a.m.?

14 A. Yes.

15 Q. 3570D appears to be an email dated Tuesday, March 10, 2009,  
16 at 11:33 a.m.?

17 A. Yes.

18 Q. And finally, 3570E appears to be an email dated Friday,  
19 May 8, 2009, at 5:21 p.m.?

20 A. Yes.

21 Q. Are these printed copies of the emails that you put into  
22 the Smith John Yahoo account and about which you testified  
23 earlier?

24 A. Yes, they are.

25 MS. GRISWOLD: The government offers 3570A through

HC5TTUZ7

DeCapua - Redirect

1 570E for the purpose of this hearing.

2 THE COURT: Any objection?

3 MR. JACKSON: No objection.

4 MS. GRISWOLD: No further questions.

5 THE COURT: All right. 3570A, B, C, D and E are  
6 received.

7 (Government's Exhibits 3570A through E received in  
8 evidence)

9 THE COURT: Anything else, Mr. Jackson?

10 MR. JACKSON: Not for this witness, thank you.

11 THE COURT: Okay, you may step down, sir.

12 Is it your intention to call Agent Amato?

13 MS. GRISWOLD: Special Agent Amato, we'll proceed if  
14 you would like to. I would request a two-minute bathroom  
15 break.

16 THE COURT: Absolutely. We'll take a brief recess.

17 (Recess)

18 (Continued on next page)

19

20

21

22

23

24

25

**In The Matter Of:**  
*UNITED STATES OF AMERICA, v.*  
*KALEIL ISAZA TUZMAN, et al.,*

---

*December 18, 2017*

---

*Southern District Court Reporters*

Original File HciWtuzF.txt  
Min-U-Script® with Word Index

HCITTUZ5	Page 6291	HciWtuz6	DeCapua - Direct	Page 6293
1 already about his relationship with Jamie Yavelberg, so I am 2 going to need to see how this impeaches something he said about 3 his relationship with Jamie Yavelberg. 4 MR. JACKSON: Your Honor, we'll pull the transcript 5 cites. It would be more efficient. Thank you. 6 MR. WILLIAMS: Your Honor, even if they could 7 establish relevance on impeachment grounds, that only address 8 the first lines of the first page. The real work that they did 9 was on the second page, the paragraphs starting with the good 10 news. To have that first sentence then link up with the last 11 sentence of the paragraph, which isn't even a full sentence, 12 the full sentence is: But the benefit of wrapping myself in 13 the ugly truth of my actions over the last five years should 14 get me home to my family soon, hopefully in the first half of 15 2018. 16 Now as a matter of just -- it should be clear that, at 17 a minimum, the way that the statement has been redacted, it 18 makes it appear that the prosecutors told Mr. Maiden that he 19 did well, and that it should hopefully get him home to his 20 family soon, when in reality he's saying I told the truth at 21 trial. 22 THE COURT: I don't think the redaction is fair. So 23 if any of this is coming in, and I haven't made any ruling on 24 that, the redactions do not strike me as fair. 25 MR. WEITZMAN: Okay. Let us talk to the government	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25	THE COURT: Please be seated. All right. Are we prepared to proceed? MS. GRISWOLD: Yes, your Honor. MR. JACKSON: Yes, your Honor. MR. LEACH: Your Honor, before we begin, would you mind formally excusing Mr. Isaza Tuzman again on the record? THE COURT: Yes. Mr. Tuzman, you don't need to be here for this hearing if you don't want to be. You're free to leave. MR. LEACH: Thank you very much, your Honor. THE COURT: Yes. Ms. Griswold, do you want to call Agent DeCapua? MS. GRISWOLD: Yes, your Honor. The government calls Special Agent Joel DeCapua. JOEL DECAPUA, called as a witness by the Government, having been duly sworn, testified as follows: THE COURT: Please proceed. MS. GRISWOLD: Thank you. DIRECT EXAMINATION BY MS. GRISWOLD: Q. You're a special agent with the FBI? A. That's correct. Q. How long have you been a special agent? A. Since 2009.	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25	
HCITTUZ5	Page 6292	HciWtuz6	DeCapua - Direct	Page 6294
1 and see if we can figure out some resolution, your Honor. 2 MR. WILLIAMS: Thank you, your Honor. 3 THE COURT: All right. We'll resume at 6:00. 4 (Recess) 5 (Continued on next page) 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25	Q. And what squad are you currently assigned to? A. I'm current am assigned to CY-2. Q. What is CY-2? What types of cases do they investigate? A. CY-2 investigates criminal network intrusions. Q. How long have you been on CY-2? A. Since 2014. Q. Prior to that, what types of cases were you investigating? A. I worked primarily securities fraud cases and public corruption cases. Q. Did those cases involve the execution of email search warrants? A. Yes, they did. Q. Can you describe the training you've received at the FBI in cyber security and digital forensics? A. Absolutely. So, it began at Quantico with the regular curriculum that all new agents are taught. We learned how to analyze packet captures and email headers and basic cyber investigation techniques. From then, from that point, once I joined the cyber squad, I took other FBI-sponsored training on how to handle digital evidence, more training on how to analyze headers and emails, training on how to conduct Internet investigations and cyber investigations in general, up to the advanced level. And I've also taken extension -- extensive training in, from private-sector nonprofits who teach cyber security, network forensics and digital forensics.	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

UNITED STATES OF AMERICA, v.  
KALEIL ISAZA TUZMAN, et al.,

December 18, 2017

HciWtuz6	DeCapua - Direct	Page 6295	HciWtuz6	DeCapua - Direct	Page 6297
1	MS. GRISWOLD: Ms. Pyun, can you pull up Special Agent		1	have that are relevant to the analysis of email evidence and in	
2	DeCapua's résumé, which I think we have marked for		2	particular email headers?	
3	identification 3539-06.		3	A. Sure. So, I would say the first one is the certified fraud	
4	I apologize, your Honor. I don't have a hard copy of		4	examiner certification, and there is a small portion where we	
5	this.		5	talk about emails and fraud investigations as it relates to	
6	THE COURT: OK.		6	digital evidence. I was, I studied and was tested on it. I	
7	MR. JACKSON: Your Honor, while we're pulling that up,		7	passed examination. My current certification is inactive,	
8	may I ask for a time frame for the Quantico training?		8	current, right now.	
9	THE COURT: A time frame?		9	Next, March 2015, the GIAC security essentials	
10	MR. JACKSON: Yes, your Honor.		10	certification, this was the entry-level network security	
11	THE COURT: What period were you at Quantico, Agent?		11	certification. I studied, was tested and credentialed on	
12	THE WITNESS: From August of 2009 until December of		12	basic -- I wouldn't call it basic. I would say intermediate to	
13	2009.		13	advanced cyber security. From there I was able --	
14	MR. JACKSON: Thank you, your Honor.		14	THE COURT: What does GIAC stand for, do you know?	
15	BY MS. GRISWOLD:		15	THE WITNESS: So, it stands for global information	
16	Q. Before we turn to your résumé, and I want to walk through		16	assurance certification, I think. It's a nonprofit company	
17	some of these forensic investigation or forensic certifications		17	that tests people and awards certifications based on knowledge	
18	that you have, you used a couple of terms in your last answer		18	as demonstrated in tests.	
19	that I just want to clarify for the record. What is a packet		19	BY MS. GRISWOLD:	
20	capture?		20	Q. And GIAC, is that a well-recognized place to go for	
21	A. So, a packet capture is when you receive raw network		21	certifications for FBI agents?	
22	communication over the wire, as we refer to it. It is ones and		22	A. Yes, for FBI agents and in general for digital forensics	
23	zeros that we can analyze and understand what type of		23	practitioners, it's considered a gold standard certification.	
24	communication is going on between a computer and a server,		24	Q. And what specifically, you said intermediate level email	
25	computer and another computer or a server and another server.		25	analysis or header analysis. Can you give us an example of the	
HciWtuz6	DeCapua - Direct	Page 6296	HciWtuz6	DeCapua - Direct	Page 6298
1	Q. You used the term "email header." Can you describe what		1	types of things you're learning when you're getting this	
2	email header is?		2	certification?	
3	A. An email header is the part of an email that reflects the		3	A. So in the GSEC certification, you're learning some basic	
4	metadata about the email. It includes the date, the "to," the		4	email header analysis. You're taught how computers communicate	
5	"from," what servers the email passed through as it was going		5	with email servers. More generally, you're taught about	
6	from the sender to the recipient and some other data points		6	network security concepts. It wasn't until the more advanced	
7	that are hidden from an end user of an email.		7	certifications that I learned more about email headers.	
8	Q. I want to turn to that in more detail, but before we do, do		8	Q. Let's talk about those.	
9	you see what is marked on the screen in front of you as		9	A. So the next one is the certified forensic examiner. This	
10	3509-06?		10	one goes into great detail on how emails are sent and received	
11	A. Yes.		11	on the network, what encompasses an email header, where to look	
12	Q. Is this a résumé you prepared?		12	to get evidence related to whether or not an email is	
13	A. It is.		13	authentic.	
14	Q. Is it an accurate summary of your career, experience, your		14	The certified intrusion analyst and certified incident	
15	certifications, training, professional affiliations and your		15	handler are additional advanced cyber security certifications	
16	education?		16	where I learned how to detect hackers and conduct	
17	A. Yes.		17	investigations related to cyber security.	
18	MS. GRISWOLD: For the purpose of this hearing, the		18	Certified forensic analyst is another certification where	
19	government would offer 3539-06.		19	we talk about digital forensics. That included email header	
20	THE COURT: Any objection?		20	analysis. Not as high detail as the GCFE certification.	
21	MR. JACKSON: No objection, your Honor.		21	The next certification, network forensic analyst, again,	
22	THE COURT: 3539-06 is received.		22	this one was very detailed in analyzing specifically how emails	
23	(Government Exhibit 3539-06 received in evidence)		23	are sent over a network and what protocols are used and where	
24	BY MS. GRISWOLD:		24	to look to gather evidence related to those emails.	
25	Q. Can you walk the Court through the certifications that you		25	The next certification was an FBI-sponsored certification.	

HciWtuz6	DeCapua - Direct	Page 6299	HciWtuz6	DeCapua - Direct	Page 6301
<p>1 We call it DexT training, digital extraction technician. It's      2 a two-week course with a test where I learned how to handle      3 digital evidence and review it and analyze it for the purposes      4 of investigations. And that is the last certification that is      5 relevant.</p> <p>6 Q. In total, approximately how much time would you approximate      7 you have spent training that is relevant to electronic      8 evidence, specifically, relevant to email headers?</p> <p>9 A. Formalized, I would say two weeks.</p> <p>10 Q. And in terms of training, based on your investigations, can      11 you describe since you've been on the cyber squad in 2014, the      12 types of cases that you have had that have involved the review      13 of electronic evidence and email headers?</p> <p>14 A. Lots of cases.</p> <p>15 Q. Can you give us an example?</p> <p>16 A. So one example would be the J.P. Morgan Chase hack of 2014.</p> <p>17 Q. And in that case, was the investigation looking at getting      18 into J.P. Morgan's systems in order to steal information?</p> <p>19 A. Yes.</p> <p>20 Q. What, if any, review of emails was involved in that case?</p> <p>21 A. The majority of the review would be from the spin-off cases      22 that resulted in initially investigating the J.P. Morgan Chase      23 hack.</p> <p>24 Q. What do you mean by that?</p> <p>25 A. So, in any normal investigation, there's the primary</p>	<p>1 Q. What is a Message-ID?</p> <p>2 A. A Message-ID is a field in an email header that is      3 invisible to the end user unless you know where to look to find      4 header information, and it -- by specification, all it is is a      5 unique number that identifies that specific email. What it has      6 become is large numbers that use specific conventions by      7 different web mail services or client-side email services that      8 allow us to look at a Message-ID and fingerprint what specific      9 service was used to send the email.</p> <p>10 Q. For example, in the hearing that we had that you previously      11 testified in this case, you gave an example that one of the      12 things a Message-ID can tell you may be the type of device,      13 Blackberry or Apple, for example, that was used to send the      14 message?</p> <p>15 A. Correct.</p> <p>16 Q. And there's other types of information that you can get      17 from Message-ID?</p> <p>18 A. There is.</p> <p>19 Q. Are you familiar with epoch time stamp?</p> <p>20 A. I am.</p> <p>21 Q. What is it?</p> <p>22 A. Epoch time stamp, also known as a Unix time stamp, is a way      23 that computers read time, and what it is is the number of      24 seconds from midnight January 1, 1970, using Greenwich Mean      25 Time, and it has become a standard way that computers</p>				
HciWtuz6	DeCapua - Direct	Page 6300	HciWtuz6	DeCapua - Direct	Page 6302
<p>1 investigation, and as you're investigating that specific      2 allegation, you find other instances of federal crimes being      3 committed, and you gather more evidence and you seek to grow      4 the case and build it out. And we analyzed emails extensively      5 for the J.P. Morgan Chase case, but also with the spin-off      6 cases it was even more so.</p> <p>7 Q. Did that involve analysis of header information?</p> <p>8 A. It did.</p> <p>9 Q. Is that sometimes referred to as metadata?</p> <p>10 A. Yes.</p> <p>11 Q. Is there a difference?</p> <p>12 A. There is a difference. Email headers are a very specific      13 thing. "Metadata" is more of a word that's used by attorneys.      14 For a forensicator, we would always refer to it as email      15 header, and other forensicators will know what email header is      16 and what it encompasses. When I'm trying to explain to an      17 attorney, I would say an email header includes what you would      18 consider metadata.</p> <p>19 Q. I want to ask you about some specific features of      20 headers --</p> <p>21 A. Sure.</p> <p>22 Q. -- and if you could describe your experience in your      23 investigations whether you have come across these items and      24 reviewed these items. Message-ID, are you familiar with that?</p> <p>25 A. I am.</p>	<p>1 communicate times to each other. So as a forensicator, there      2 is human readable times, like March 2, 2009, and then there are      3 computer readable times, such as epoch time.</p> <p>4 THE COURT: How do you spell that?</p> <p>5 THE WITNESS: Epoch is E-P-O-C-H, and Unix is U-N-I-X.</p> <p>6 BY MS. GRISWOLD:</p> <p>7 Q. And in the course of the investigations that you have had      8 since you've been on the FBI cyber squad, have you had occasion      9 to review Message-IDs, epoch time and epoch time stamps?</p> <p>10 A. Yes, separately, but never combined.</p> <p>11 Q. Sorry. I should have asked them separately.</p> <p>12 You've reviewed Message-IDs?</p> <p>13 A. I have.</p> <p>14 Q. And you've reviewed epoch time stamps?</p> <p>15 A. I have.</p> <p>16 Q. Have you had training at the FBI in connection with your      17 review of these items?</p> <p>18 A. Yes.</p> <p>19 Q. Are you familiar with the term "web mail"?</p> <p>20 A. I am.</p> <p>21 Q. What does it mean?</p> <p>22 A. Web mail is a service like GMail or Yahoo or HotMail. It's      23 a place where you can open up an account, log in, and send and      24 receive emails that is generally hosted on a remote server.</p> <p>25 Q. Approximately how many web mail accounts have you been</p>				

HciWtuz6	DeCapua - Direct	Page 6303	HciWtuz6	DeCapua - Direct	Page 6305
<p>1 involved in reviewing over the course of your career?</p> <p>2 A. Hundreds.</p> <p>3 Q. Does that include accounts listed by Yahoo?</p> <p>4 A. Yes.</p> <p>5 Q. Have you become familiar with what is known as a local</p> <p>6 email client?</p> <p>7 A. Yes.</p> <p>8 Q. What is a local email client?</p> <p>9 A. A local email client is like Outlook or Apple Mail or</p> <p>10 Thunderbird, and instead of having to log in to a remote server</p> <p>11 to send or receive emails, it allows you to connect with a</p> <p>12 remote server from your own computer and send and receive and</p> <p>13 store emails.</p> <p>14 Q. And in the course of your work at the FBI, have you become</p> <p>15 familiar with how, if at all, a web mail account and local</p> <p>16 email client can interact with one another?</p> <p>17 A. Yes.</p> <p>18 Q. Can you explain that?</p> <p>19 A. So, I learned about the different protocols that a local</p> <p>20 email client and a web server would use to talk to each other.</p> <p>21 There's three primary ones, POP, POP3, and IMAP.</p> <p>22 THE COURT: Could you spell those for us.</p> <p>23 THE WITNESS: So POP is P-O-P. POP3 is P-O-P-3, and</p> <p>24 IMAP is I-M-A-P.</p> <p>25 And as a protocol, it's just an agreed-upon language</p>	<p>1 whether you're at work or you're at home, you want to be all</p> <p>2 looking at the same emails and IMAP works to synchronize this.</p> <p>3 Q. So if you have the settings in IMAP set to synchronize</p> <p>4 between your local email client and your web mail account,</p> <p>5 would that mean changes that you might make in your local email</p> <p>6 client would be reflected in the web mail account?</p> <p>7 A. Yes.</p> <p>8 Q. Are you familiar in the course of your FBI training and</p> <p>9 investigations with the term "spoofing"?</p> <p>10 A. I am.</p> <p>11 Q. What does it mean?</p> <p>12 A. Spoofing generally means tampering with an email header to</p> <p>13 either make an email look like it's not from who it says it</p> <p>14 is -- or, I'm sorry. Let me -- What I mean is, it's to make an</p> <p>15 email look like it's from someone other than who it's actually</p> <p>16 from, or it can be used to change the date on an email, or you</p> <p>17 could spoof on email to change the recipients, or you can spoof</p> <p>18 an email to change the content of the email.</p> <p>19 Basically, it means taking a raw email and spoofing some</p> <p>20 portion of it.</p> <p>21 Q. And have you had training about spoofing at the FBI?</p> <p>22 A. I have.</p> <p>23 Q. And in fact, is spoofing an area of focus for the FBI</p> <p>24 currently?</p> <p>25 A. It is, particularly in the realm of business email</p>				
HciWtuz6	DeCapua - Direct	Page 6304	HciWtuz6	DeCapua - Direct	Page 6306
<p>1 that a server and your personal computer are going to use to</p> <p>2 transmit information. The most popular used protocol right now</p> <p>3 is IMAP, which among other things, allows the synchronization</p> <p>4 of emails between your personal home computer with Outlook or</p> <p>5 Apple Mail and a remote email server, such as GMail or HotMail,</p> <p>6 or your work's email server.</p> <p>7 BY MS. GRISWOLD:</p> <p>8 Q. And in your work at the FBI, have you become familiar with</p> <p>9 how POP, POP3 and IMAP function?</p> <p>10 A. I have.</p> <p>11 Q. And in particular, focusing you on IMAP, can you explain</p> <p>12 how IMAP functions?</p> <p>13 A. So, very generally, IMAP, as I mentioned before, is an</p> <p>14 agreed-upon way that your computer's going to speak to a remote</p> <p>15 server, and in general, IMAP has a function where it will look</p> <p>16 on the remote server and determine whether it contains anything</p> <p>17 that is not on your personal computer, and if there's an email</p> <p>18 that was received by remote server but not received by your</p> <p>19 computer at home, via IMAP it will pull that email down and</p> <p>20 sync with your home computer. And it also works in the reverse</p> <p>21 manner, which if there is something, if there's an email on</p> <p>22 your home computer that doesn't exist on a remote server, it</p> <p>23 will sync and make sure everything has the same emails.</p> <p>24 It does this, it's out of convenience. You want to have</p> <p>25 your emails wherever you go, and however you access them,</p>	<p>1 compromises.</p> <p>2 Q. In total, how many headers, email headers have you reviewed</p> <p>3 in the course of your time on the FBI cyber squad?</p> <p>4 A. Hundreds.</p> <p>5 Q. And how many times have you observed accounts, local email</p> <p>6 client accounts and web mail accounts synchronized?</p> <p>7 A. I -- it's hard to put a number on it, but a handful of</p> <p>8 time.</p> <p>9 MS. GRISWOLD: At this time, the government seeks to</p> <p>10 qualify Special Agent DeCapua as an expert in email analysis.</p> <p>11 MR. JACKSON: I don't know that that's necessary for</p> <p>12 this hearing, your Honor.</p> <p>13 THE COURT: All right. I find based on the record</p> <p>14 that's been laid that he is an expert in email analysis.</p> <p>15 BY MS. GRISWOLD:</p> <p>16 Q. Special Agent DeCapua, based only on the fact that an email</p> <p>17 appears in a web mail account, only on that fact and based on</p> <p>18 your training and experience, are you able to offer an opinion</p> <p>19 that an email is authentic?</p> <p>20 A. No.</p> <p>21 Q. Why not?</p> <p>22 A. Because emails are not self-authenticating. If you have</p> <p>23 access to a Yahoo account, you can put anything into it you</p> <p>24 want, as I demonstrated at the hearing before, just by</p> <p>25 tampering with the header information or the content of an</p>				

UNITED STATES OF AMERICA, v.  
KALEIL ISAZA TUZMAN, et al.,

December 18, 2017

HciWtuz6	DeCapua - Direct	Page 6307	HciWtuz6	DeCapua - Direct	Page 6309
1	email and then synchronizing it through a local email client to		1	A. Yes.	
2	a remote server.		2	Q. Were you also given access to search warrant results for a	
3	Q. And I want to be clear, when you say if you have access; we		3	GMail account for irfan.amanat@gmail.com?	
4	talked about the term "hacking" both in your prior testimony		4	A. Yes.	
5	and today. When you say have access, do you mean hacking or do		5	Q. Based on those different sources of information, what, if	
6	you mean something else?		6	anything, did you identify about the header information that	
7	A. No. I mean, it's your account, you use your password to		7	7 you then relayed to the government?	
8	access it, or it could be someone else's account where you have		8	A. So, I was looking for a way to show the authenticity of	
9	their password, but in my demonstration, it was an account that		9	this email just by using technical means, just by looking at	
10	I created with my password.		10	the header information, and one thing -- there isn't a lot to	
11	Q. And does the term "hacking" typically connote going into		11	work with here. And one thing I zoomed in on was the	
12	someone else's database or account?		12	Message-ID.	
13	A. It does, yes.		13	Q. Is that highlighted there on the screen?	
14	Q. OK. Now I want to turn to, you testified in a previous		14	A. It is.	
15	hearing with the focus on an email dated May 8, 2009. Do you		15	Now, as I mentioned before, a Message-ID, there's no	
16	remember that?		16	standard for what it's supposed to look like; it just has to be	
17	A. Yes.		17	unique, but every company has their own unique twist or spin on	
18	Q. And this past weekend, were you asked to go back and look		18	how they create Message-IDs. And this one is for a Blackberry	
19	at three additional emails again and particularly the header		19	device, and looking at it, I hypothesized that there is maybe	
20	information?		20	some data in here that I'm missing. So what I did is I looked	
21	A. I was.		21	at other Message-IDs that were in the body of evidence for this	
22	MS. GRISWOLD: If we could pull up on the screen, I		22	case, in the GMail account and then on the Maiden computer, and	
23	don't have hard copies, to begin with, Government Exhibit 3550		23	I took all the Message-IDs that were sent from	
24	and 908 side by side, please, Ms. Pyun.		24	omar@amanatcapital.com and also had a Message-ID that	
25	THE COURT: 908 is Amanat 908.		25	referenced a Blackberry device, and I just looked at them all	
HciWtuz6	DeCapua - Direct	Page 6308	HciWtuz6	DeCapua - Direct	Page 6310
1	MS. GRISWOLD: I'm sorry. Amanat Exhibit 908 and		1	together to see if I could find any obvious patterns.	
2	Government Exhibit 3550.		2	Q. And approximately how many in total, just in order of	
3	May Mr. Urbanczyk approach, your Honor?		3	magnitude?	
4	THE COURT: Yes.		4	A. Hundreds.	
5	MS. GRISWOLD: Thank you.		5	Q. Hundreds of messages?	
6	THE COURT: Thank you.		6	A. Over a long period of time, years.	
7	BY MS. GRISWOLD:		7	Q. And you reviewed hundreds?	
8	Q. On the left, the document that's in evidence from the prior		8	A. Yes.	
9	hearing is Government Exhibit 3550, do you see that as an email		9	Q. OK. Go ahead.	
10	with header information on the top that appears to be dated		10	A. And I found a very obvious pattern in the Message-ID that	
11	March 10, 2009?		11	indicated to me that the Message-ID has a hidden time stamp	
12	A. I do.		12	that tells you the date the email was sent.	
13	Q. And do you understand this to be header information that		13	MS. GRISWOLD: I'm going to pass up what is marked for	
14	was provided to the government by the defendant in this case?		14	identification as Government Exhibit 3579-A, we can give a hard	
15	A. That's correct.		15	copy to the Court, and we have one for Mr. Jackson too.	
16	Q. And on the right, Amanat Exhibit 908, do you understand		16	Q. Do you recognize this, Special Agent DeCapua, as a chart	
17	this to be in evidence as an exhibit that was offered in this		17	that you prepared this evening based on the information that	
18	case?		18	you obtained?	
19	MS. GRISWOLD: I'll strike that question.		19	A. Yes.	
20	Q. Focusing on 3550, did you take a closer look at this header		20	Q. Is it accurate?	
21	information over the weekend?		21	A. Yes.	
22	A. I did.		22	MS. GRISWOLD: The government offers 3579-A.	
23	Q. And were you given access to emails on computers that an		23	MR. JACKSON: For the purposes of the hearing, we have	
24	individual named Stephen Maiden had turned over to the FBI in		24	an objection, your Honor. We haven't been provided with this	
25	2013?		25	in advance or any of the underlying data associated with it.	

HciWtuz6	DeCapua - Direct	Page 6311	HciWtuz6	DeCapua - Direct	Page 6313
1	MS. GRISWOLD: Just to be clear, the underlying data		1	THE WITNESS: That's correct, which would be Greenwich	
2	is on Mr. Maiden's computer and Irfan's GMail account and in		2	Mean Time.	
3	the header information provided from the defendant. It is true		3	BY MS. GRISWOLD:	
4	that the chart was just provided.		4	Q. So taking the first row --	
5	THE COURT: All right. Well, I'll receive the exhibit		5	MS. GRISWOLD: We can pop back out, Ms. Pyun.	
6	for purposes of the hearing.		6	Q. -- the very first row, am I correct, is just an email that	
7	(Government Exhibit 3579-A received in evidence)		7	you found on Mr. Maiden's computer from Omar --	
8	BY MS. GRISWOLD:		8	THE COURT: I'm sorry. Before we leave the hidden	
9	Q. This is titled "select emails present on Stephen Maiden's		9	time stamp, and maybe you've already said this, how do you find	
10	computer around March 10, 2009, sent from Omar Amanat with a		10	the hidden time stamp? Is that in a Message-ID or someplace	
11	Blackberry Message-ID"?		11	else?	
12	A. Yes.		12	THE WITNESS: So having analyzed hundreds of epoch	
13	Q. Can you explain, and there's a lot on this chart, but going		13	time stamps, I know that they start with either 1-2 or 1-3, and	
14	column by column what it is that you identified?		14	I know the approximate size. And when I was looking at the	
15	A. So, the first column is the dates and time as indicated on		15	Message-IDs, I saw that the second number -- do you see there's	
16	the face of the email. The second column is the sender, which		16	a first number.	
17	is always Omar Amanat. The third column is the Message-ID, and		17	THE COURT: Yes.	
18	the fourth column is the hidden time stamp, which is an epoch,		18	THE WITNESS: Then the second number.	
19	or Unix, time stamp. And the fifth column is the conversion		19	THE COURT: Yes.	
20	that I made from the epoch time stamp to a human readable time		20	THE WITNESS: First I saw the second number was	
21	and date.		21	incrementing as date goes by, and then it was obvious to me,	
22	Q. What do you use to make that conversion?		22	This is an epoch time stamp, how did I miss this?	
23	A. There are online tools that allow you to do it. It's		23	THE COURT: OK. Go ahead, Ms. Griswold.	
24	mathematics. The time stamp is a number of seconds, and you		24	BY MS. GRISWOLD:	
25	can assume 365 days in a year, 24 hours a day --		25	Q. So taking the first row which we know to be an email on	
HciWtuz6	DeCapua - Direct	Page 6312	HciWtuz6	DeCapua - Direct	Page 6314
1	Q. So it's a formula?		1	Mr. Maiden's computer, correct?	
2	THE COURT: I'm sorry?		2	A. That's correct.	
3	MS. GRISWOLD: I'm sorry. I was just asking if it's a		3	Q. You took the hidden time stamp that you found that begins	
4	formula.		4	with 1233, and you ran it through the formula and it gave you	
5	THE COURT: OK. It's going to be hard for the court		5	January 27, 2009, is that correct?	
6	reporter to get this all down if you're both speaking at the		6	A. That's correct.	
7	same time, so if you could pick up where you were interrupted.		7	Q. Which matches, if we go to the column all the way on the	
8	THE WITNESS: There's a formula where you can convert		8	left, the date that appears, the date and time that appears on	
9	this time stamp, which represents a number of seconds of a		9	the actual email, aside from the header information, is that	
10	specific date into a human readable date that looks familiar to		10	correct?	
11	us.		11	A. That's correct.	
12	THE COURT: Now, is this tied to the January 1, 1970,		12	Q. And was that the case for the hundreds of emails that you	
13	date that you mentioned earlier?		13	reviewed that came from Omar's Blackberry account?	
14	THE WITNESS: Yes.		14	A. Yes.	
15	THE COURT: How does the hidden time stamp relate to		15	Q. And then focusing on the highlighted one --	
16	that date?		16	MS. GRISWOLD: If we can highlight that one, Ms. Pyun.	
17	THE WITNESS: It's the number of seconds that have		17	Q. -- how was this one different?	
18	elapsed since midnight, January 1, 1970, and it's something		18	A. This was the email that was provided by the defendant, and	
19	that's widely used in computer networking.		19	when I converted the hidden time stamp, it came to July 23,	
20	THE COURT: This is just arithmetic. You figure out		20	2009, which is obviously different than the stated sent date on	
21	how many seconds equals how many hours equals how many days		21	the email.	
22	equals how many weeks, etc.?		22	Q. Which is March 10, 2009?	
23	THE WITNESS: That's exactly right.		23	A. Correct.	
24	THE COURT: And that in this case brings you to July		24	Q. Did you discuss this finding with colleagues at the FBI?	
25	23, 2009, at 19 minutes past midnight.		25	A. I did.	

UNITED STATES OF AMERICA, v.  
KALEIL ISAZA TUZMAN, et al.,

December 18, 2017

HciWtuz6	DeCapua - Direct	Page 6315	HciWtuz6	DeCapua - Direct	Page 6317
1	Q. And were they familiar with this hidden time stamp feature?		1	words, was the email actually sent on July 23, 2009, at 19	
2	A. No.		2	minutes after midnight, or we just don't know?	
3	Q. Based on your review of the Message-IDs for this particular		3	THE WITNESS: The only thing that I can draw from that	
4	email and your review of all of the sample size from		4	is someone changed the header or the content before they gave	
5	Mr. Maiden's computer and Mr. Irfan Amanat's GMail account, are		5	it to us. Someone changed it. It is not the authentic,	
6	you able to offer an opinion as to whether or not this email is		6	original email. What I assume happened is that the email that	
7	authentic?		7	was used to spoof the header was actually sent on July 23,	
8	A. Yes. It's fake.		8	2009, at 19 minutes after midnight GMT, and that header was	
9	THE COURT: Is that simply because the date and time		9	copied and pasted and then someone went through and changed all	
10	of column 1 doesn't match up with the time stamp conversion in		10	the things that they thought were relevant, like the date and,	
11	the last column?		11	you know, perhaps the subject line or anything else they wanted	
12	THE WITNESS: That's correct.		12	13 to change, content, but they didn't realize this hidden time	
13	BY MS. GRISWOLD:		13	stamp existed and therefore they didn't change it.	
14	Q. Special Agent DeCapua, at your last testimony, you		14	THE COURT: OK.	
15	testified a lot about that May 8, 2009 email, correct?		15	MS. GRISWOLD: If we could put up on the screen	
16	A. Yes.		16	Government Exhibit 3552 from the hearing and Amanat Exhibit	
17	Q. And you told the Court about certain facial abnormalities		17	9002.	
18	that raised some suspicion for you?		18	Q. The next email that you looked at, Special Agent DeCapua,	
19	A. Yes.		19	an email dated Wednesday, December 3, 2008, or rather, I guess	
20	Q. And you testified about one Message-ID that appeared to be		20	the Tuesday, December 2, 2008, email at 11:07 p.m.?	
21	sent from an Apple that seemed odd compared to some		21	A. Yes.	
22	Blackberries?		22	Q. And on the left side of your screen, Government Exhibit	
23	A. Correct.		23	3552, do you understand this to be the version provided to the	
24	Q. And you testified that that email wasn't in certain of the		24	government by the defendant that contained the header	
25	accounts for the participants on the email?		25	information?	
HciWtuz6	DeCapua - Direct	Page 6316	HciWtuz6	DeCapua - Direct	Page 6318
1	A. That's correct.		1	A. Yes, I do.	
2	Q. And yet you were still cautious to say that -- you wouldn't		2	Q. What did you notice about this header?	
3	say with a reasonable degree of scientific certainty that that		3	A. So, like the one before it, I noticed the Message-ID is	
4	email was fake; do you recall that question on		4	consistent with Message-IDs sent from BlackBerry devices. The	
5	cross-examination?		5	one thing that really struck me is the hidden time stamp, that	
6	A. I do.		6	number is actually a time in the future when I do the	
7	Q. And yet you are saying that your opinion is that this email		7	conversion, and it was very much out of place.	
8	is fake?		8	MS. GRISWOLD: If we could put up what's marked for	
9	A. That is correct.		9	identification as Government Exhibit 3579-B.	
10	Q. Why are you so positive?		10	Q. Do you recognize this as a chart that was prepared relating	
11	A. Because this is -- this is something that would be so easy		11	12 to emails on December 2, 2008, that was prepared this evening?	
12	for someone who is spoofing an email to overlook. When you're		12	A. Yes.	
13	looking at a Message-ID, you don't realize there's an embedded		13	Q. Is this accurate?	
14	time stamp. It's easy to spoof the date in the header of an		14	A. It is.	
15	email, because you just type a different date, as I did in my		15	MS. GRISWOLD: The government offers for the purposes	
16	demonstration. But this is something that is very easy to		16	of this hearing Government Exhibit 3579-B.	
17	overlook, and it's something that's very concrete. Of all the		17	MR. JACKSON: No objection.	
18	other emails I've looked at, they were completely consistent		18	THE COURT: 3579-B is received for purposes of the	
19	this time stamp reflects the sent date of an email, with two		19	hearing.	
20	exceptions, and this email is the first exception.		20	(Government Exhibit 3579-B received in evidence)	
21	Q. Let's go --		21	BY MS. GRISWOLD:	
22	THE COURT: Before we leave this, with respect to the		22	Q. Can you walk us through 3579-B, please?	
23	highlighted email on Government Exhibit 3579-A, the time stamp		23	A. So it has the same fields as the previous spreadsheet.	
24	conversion comes out at July 23, 2009, 19 minutes after		24	This one only includes the email that was sent on December 2,	
25	midnight. What, if anything, can we draw from that? In other		25	2008, that was provided by defendant, and I included the time	

HciWtuz6	DeCapua - Direct	Page 6319	HciWtuz6	DeCapua - Direct	Page 6321
1	frame that that email was sent from the emails I found in the		1	DeCapua?	
2	Maiden account.		2	A. Yes, it is.	
3	Q. And the converted time stamp converts to October 29, 2087?		3	Q. And that 3551 is the email provided by the defendant that	
4	A. That's correct.		4	contained the header information?	
5	And I might add specifically for this one, it was so		5	A. That's correct.	
6	different than all the rest that I tried to come up with		6	Q. What did you identify about this email?	
7	alternative hypotheses of why this possibly could be, and aside		7	A. Looking at this email's header information, I noticed that	
8	from Unix time stamps, there's other types of time stamps that		8	it is not a Blackberry email, like the ones before it. This	
9	exist that use different dates as their epoch, not January 1,		9	one actually follows the convention of an Apple Mail email	
10	1970, and I ran those calculations. I ran calculations that		10	service, and I noticed the Message-ID was something that is	
11	assumed that the hidden time stamp is actually hexadecimal,		11	referred to in computer science as a UUID.	
12	which I think we're going to talk about later, but it's another		12	THE COURT: As a what?	
13	way to store time stamps.		13	THE WITNESS: UUID.	
14	THE COURT: Could you spell that for the record,		14	It stands for universal unique identifier. And it's a	
15	please.		15	very well defined, specific type of number. It is, the format	
16	THE WITNESS: H-E-X-I-D-E-C-I-M-A-L.		16	of it looks like this. It is eight digits and a dash, four	
17	THE COURT: And what does hexadecimal mean?		17	digits, a dash, four more digits, another dash, four more	
18	THE WITNESS: Hexadecimal is a base-16 way of counting		18	digits, a dash and then 12 digits.	
19	used by computers. It's basically the digits zero through 9		19	BY MS. GRISWOLD:	
20	and A through F, F being 16, A being 10, zero being zero. And		20	Q. And that's on the face of the Message-ID; you don't need to	
21	computers, particularly when speaking about networking, can		21	look for anything hidden in this one, correct?	
22	store a lot of information in hex. And sometimes you'll find		22	A. That's correct.	
23	time stamps that are stored in hex. And this number,		23	Q. And what did you notice about this Message-ID?	
24	3718305712, it meets the specification that it could be hex,		24	A. I know that all UUIDs are in hexadecimal, which we talked	
25	and I tried the various different types of hex conversions to		25	about before, and the only possible characters is hexadecimal	
HciWtuz6	DeCapua - Direct	Page 6320	HciWtuz6	DeCapua - Direct	Page 6322
1	convert it to a time stamp. None of those conversions were		1	are zero through 9 and A through F, and I noticed that in this	
2	December 2, 2008. None were in the ballpark. Some were in the		2	UUID there's a character V.	
3	future, some were in the past, but none in the ballpark of when		3	THE COURT: Character B?	
4	this email was purportedly sent.		4	THE WITNESS: V, as in Victor.	
5	BY MS. GRISWOLD:		5	THE COURT: Oh, V. Sorry.	
6	Q. And just to be clear, this chart has maybe a dozen or two		6	THE WITNESS: There's two characters V, which are	
7	rows on it. Is this just a representative sample of the emails		7	impossible in hex. They're impossible in UUIDs.	
8	that you reviewed from Mr. Maiden's computer?		8	THE COURT: When you say impossible, could you tell us	
9	A. Yes.		9	what you mean by that?	
10	Q. You said in total you reviewed hundreds of emails that came		10	THE WITNESS: In a UUID, you expect it to be a very	
11	from the omar@amanatcapital.com from the Blackberry?		11	standardized hexadecimal number in the format that's	
12	A. Yes.		12	represented here, and it could be any combination of numbers	
13	Q. In the course of that review, were these the only two		13	and letters, as long as it's zero through 9 and A through F.	
14	emails that had an epoch time stamp that didn't align with the		14	So when I find a V, something that doesn't meet that	
15	date and time the emails were sent?		15	specification, I know that it is something that is probably	
16	A. Yes.		16	tampered with.	
17	Q. Based on this information, are you able to offer an opinion		17	BY MS. GRISWOLD:	
18	based on whether or not this email is authentic?		18	Q. When you say probably, could you, are you able to offer an	
19	A. Yes. It's fake.		19	opinion based on this Message-ID as to whether or not this	
20	MS. GRISWOLD: If we could put up on the screen what's		20	email is fake or real?	
21	in evidence at the hearing as Government Exhibit 3551 and then		21	A. Yes. It's fake, and I might add that I went back and I	
22	Amanat exhibit 9013.		22	looked through all the Apple Mail IDs I could possibly look	
23	THE COURT: That's 9013, right?		23	for, and I know that it was -- it uses a UUID for it its	
24	MS. GRISWOLD: 9013, yes, your Honor.		24	Message-ID, and all the ones I looked at were consistent with	
25	Q. Is this the third email that you looked for, Special Agent		25	that, including all the research I did into this issue.	

UNITED STATES OF AMERICA, v.  
KALEIL ISAZA TUZMAN, et al.,

December 18, 2017

HciWtuz6	DeCapua - Direct	Page 6323	HciWtuz6	DeCapua - Direct	Page 6325
1	Q. And when you say you've looked at it, you're not just		1	A. No, we did not get header information for this email.	
2	talking about Maiden's computer; what did you look at for your		2	Q. So were you able to look at the Message-ID for this email?	
3	sample sizes, looking at Apple Mail's Message-ID to confirm		3	A. No.	
4	that you're right that it's only A thru F?		4	Q. Do you understand that the government asked the defendant	
5	A. So, I looked at other search warrant returns from cases		5	to provide the message -- the header information for this	
6	just to specifically look for Message-ID to see if there's any		6	email?	
7	type of deviation where a UUID might have a character that was		7	A. Yes.	
8	not hex, and I didn't find any.		8	Q. And that that request was declined?	
9	Q. And did you discuss this A-through-F concept with your		9	A. Yes, as well as access to the entire account was also	
10	colleagues at the FBI?		10	declined.	
11	A. I did. I discussed it with multiple computer scientists on		11	MS. GRISWOLD: No further questions.	
12	my floor and other agents, and we can't come up with any type		12	MR. JACKSON: Just to clarify the record, your Honor,	
13	of explanation for why this would happen other than the email		13	what we told the government is that that particular email was	
14	is tampered with.		14	not accessible, and so we didn't have header information for	
15	Q. There was complete agreement that you can't have a V in a		15	it.	
16	Message-ID for a hex?		16	THE COURT: OK. And when you say that email, you mean	
17	A. You can have a V in a Message-ID, but when you see it in		17	Amanat Exhibit 9010.	
18	this format, you know that it is a UUID, and you can't have a V		18	MR. JACKSON: I mean the underlying email that is	
19	in a UUID.		19	contained within 9010 from the Amanat account.	
20	Q. So the formatting for this Message-ID does not include the		20	THE COURT: Right.	
21	letter V, is that correct; it's not an option?		21	All right. Cross-examination.	
22	A. It's not an option for a UUID.		22	MR. JACKSON: Your Honor, I can start	
23	Q. Thank you.		23	cross-examination, but I'm going to potentially need a little	
24	MS. GRISWOLD: Finally, if we could put up on the		24	time, but I'd like to start cross-examination.	
25	screen Amanat Exhibit 9010.		25	THE COURT: OK. Let me ask a question, Mr. Jackson,	
HciWtuz6	DeCapua - Direct	Page 6324	HciWtuz6	DeCapua - Cross	Page 6326
1	THE WITNESS: One other thing I might want to add.		1	before you get started.	
2	MS. GRISWOLD: Sure.		2	Ms. Griswold, I take it there is not going to be	
3	THE WITNESS: Message-IDs have to be unique. That's		3	anything additional in terms of planting fake emails in Yahoo,	
4	the one --		4	right?	
5	THE COURT: They have to be what?		5	MS. GRISWOLD: I mean, no, your Honor. I think that	
6	THE WITNESS: Unique.		6	your Honor made clear your views and I think we made clear our	
7	THE COURT: Unique.		7	views on the demonstration about pulling them down. He has his	
8	THE WITNESS: That's the one specification that holds		8	laptop, if your Honor would like to see anything.	
9	true, and the gold standard for detecting if an email is		9	THE COURT: No, I don't need to see it again. I just	
10	spoofed is finding two emails with the same Message-ID. So		10	wanted to make sure that there wasn't anything else on that	
11	when you're going in and you want to spoof an email, you want		11	point. That's all.	
12	to change the Message-ID to something different than what the		12	MS. GRISWOLD: Thank you.	
13	original email had, and looking at this, to me, it looks like		13	THE COURT: Go ahead, Mr. Jackson.	
14	someone tried to change the original Message-ID without		14	MR. JACKSON: Thank you, your Honor.	
15	realizing that it had to be the hexadecimal format.		15	CROSS-EXAMINATION	
16	MS. GRISWOLD: Put up Amanat Exhibit 9010, please.		16	BY MR. JACKSON:	
17	Q. This is an email in evidence that is dated Thursday, June		17	Q. Good evening, Special Agent DeCapua.	
18	2, 2011. Do you see that?		18	A. Good evening.	
19	A. I do.		19	Q. Special Agent DeCapua, with regard to the first	
20	Q. And are you --		20	characteristic of a Message-ID and a Blackberry that you	
21	THE COURT: Just for the record, this is 9010.		21	discussed, you were talking about the hidden time stamp that	
22	Go ahead, Ms. Griswold.		22	you discovered?	
23	MS. GRISWOLD: Thank you, your Honor.		23	A. That's correct.	
24	Q. Is this an email for which you understand header		24	Q. Are you aware of any literature that confirms that this	
25	information was provided to the government?		25	hidden time stamp exists?	

UNITED STATES OF AMERICA, v.  
KALEIL ISAZA TUZMAN, et al.,

December 18, 2017

HciWtuz6	DeCapua - Cross	Page 6327	HCITTUZ7	DeCapua - Cross	Page 6329
1	A. No.		1	THE COURT: It held true through your analysis of	
2	Q. Did you attempt to determine whether or not there is any		2	hundreds of emails you testified.	
3	literature that suggests that this hidden time stamp was used?		3	THE WITNESS: Yes.	
4	A. I did.		4	THE COURT: Okay. Go ahead, Mr. Jackson.	
5	Q. What happened?		5	MR. JACKSON: Thank you, your Honor.	
6	A. I couldn't find any.		6	BY MR. JACKSON:	
7	Q. Were you able to find any information online at all that		7	Q. Now Special Agent DeCapua, first of all, to be clear,	
8	suggested this hidden time stamp existed in Blackberry		8	you're not an engineer, right?	
9	messages?		9	A. An agent here?	
10	A. I don't think so, no.		10	Q. Sorry, an engineer.	
11	THE COURT: Let me ask you this. Given that you're		11	A. No, I'm not, no.	
12	not aware of any literature on this, how was it that you came		12	Q. And you don't have any training in computer science,	
13	to this method of analysis? Is this something that you had		13	correct?	
14	used before in your investigations? How did this come to you?		14	A. I do have training in computer science.	
15	For example, you've given us a lot of information		15	Q. Let me back up. You don't have a degree in computer	
16	about Message-IDs and how you can tell a Blackberry email, for		16	science, right?	
17	example, from an Apple email. If there's no literature that		17	A. I don't have a degree.	
18	tells you about these hidden time stamps, how did you know		18	Q. You don't have any degrees in coding?	
19	this? How did you know how to do this?		19	A. I don't.	
20	THE WITNESS: So, two reasons. There is literature		20	Q. And I think you said the total amount of training that you	
21	that says that some companies will bake in a time stamp in the		21	have had in term of formalized training in this area amounted	
22	Message-ID. It just isn't immediately apparent. Companies		22	to about two weeks, right?	
23	don't publish anything saying they do it; you just have to kind		23	A. That's for studying email headers.	
24	of find it.		24	Q. For studying email headers amounts to about two weeks,	
25	THE COURT: So the companies don't broadcast the fact		25	right?	
HciWtuz6	DeCapua - Cross	Page 6328	HCITTUZ7	DeCapua - Cross	Page 6330
1	there's a hidden time stamp, but there's literature in which		1	A. Yes.	
2	this is referred to.		2	Q. And just to be clear, you haven't ever had any	
3	THE WITNESS: Yes.		3	conversations -- well, you haven't had any specific training on	
4	THE COURT: OK.		4	the way that Blackberry devices, different Blackberry devices	
5	THE WITNESS: And the second --		5	generate message IDs, correct?	
6	THE COURT: You said the second?		6	A. Right.	
7	THE WITNESS: The second reason is I hypothesized that		7	Q. So in terms of whatever mechanism, whatever coding	
8	there was going to be something in the Message-IDs that I could		8	mechanism a Blackberry device is using in order to generate a	
9	make sense of, and when I compared it to all the other ones, I		9	message ID, you're not personally familiar with that, right?	
10	saw the pattern and I immediately recognized it as an epoch		10	A. Other than through the use of observation and testing, no.	
11	time stamp. And then after testing it and converting it, it		11	Q. So let me ask you this, in terms of the hidden time stamp	
12	held true.		12	that you theorize is within these message IDs --	
13	(Continued on next page)		13	MR. JACKSON: Actually let me back up just one moment,	
14			14	your Honor.	
15			15	Before I circle back to that, could we take a look	
16			16	again at Government Exhibit 3551.	
17			17	Q. Now there's a message ID at the top of Government	
18			18	Exhibit 3551, right?	
19			19	A. That's correct.	
20			20	Q. And this is the message ID, Special Agent DeCapua, that you	
21			21	were looking at?	
22			22	A. Yes.	
23			23	Q. And one of the things that I think you said is this in a	
24			24	hexadecimal format?	
25			25	A. That's correct.	

UNITED STATES OF AMERICA, v.  
KALEIL ISAZA TUZMAN, et al.,

December 18, 2017

HCITTUZ7	DeCapua - Cross	Page 6331	HCITTUZ7	DeCapua - Cross	Page 6333
1 Q. And within a hexadecimal format, only the letters A through 2 F will typically appear? 3 A. That's all that will appear. 4 Q. In terms of -- as far as the type of device that is 5 created -- sorry, that is associated with a particular message 6 ID, it is possible for you to determine what the likely type of 7 device is, correct? 8 A. That's correct. 9 Q. But there is nothing that says that a different type of 10 program can't create a similar looking message ID to the type 11 of message ID that is used, for example, by Apple mail, right? 12 A. That's correct. 13 Q. This is a decision made by the programmers associated with 14 any particular email program, right? 15 A. Yes. 16 Q. It's also possible that a message ID could use a format 17 that looks like what you're describing, the hexadecimal, but 18 was not actually a hexadecimal? 19 A. It's possible. 20 Q. Okay. By the way, what does hexadecimal mean, if you can 21 enlighten us? 22 A. So we use a counting system one through ten, it's a base 23 ten counting system. However, with computers everything is 24 based on a binary circuit, and processor architecture means 25 that everything is either one or zero. And so the best way	1 always be at some point in the future. Right? 2 You haven't confirmed with anyone at Blackberry about 3 what other possibilities exist within their computing 4 infrastructure that could potentially explain this, have you? 5 A. No. 6 Q. When was it that you first notified the government about 7 this theory that you had? 8 A. It was this morning, in the early hours of the morning, I 9 believe, like 1:30 a.m. 10 Q. And when was it that you first began exploring the 11 possibility here? 12 A. Probably around 7 to 8:00 p.m. yesterday. 13 Actually, if I could make correction, I sent an email 14 to the prosecutors in early morning. I informed them of what I 15 had found, it would have been yesterday evening. And I would 16 have began this analysis sometime in the afternoon, probably 17 closer to 4:00 p.m. 18 Q. Okay. Now one of the things that you said with regard to, 19 for example, the email that is contained in Government 20 Exhibit 3551 is that your conclusion is that it's fake based on 21 the analysis you described on your direct examination, right? 22 A. That's correct. 23 Q. But putting aside -- well, let me ask you this, that is the 24 fact that the message ID is different from what you would 25 expect for a hexadecimal ID can't definitively show you that				
HCITTUZ7	DeCapua - Cross	Page 6332	HCITTUZ7	DeCapua - Cross	Page 6334
1 computers count are, instead of using base ten, it's up to 16, 2 a nice even number. And normally with computers, hexadecimal 3 is represented with ones and zeros, but to make it a little 4 more understandable for us, they designate letters to represent 5 values. And the letters continue on up through 10 up to 16, 6 and as I said, A is ten, B is eleven, all the way up to F, 7 which is 16. 8 Q. Now just turning back to the question of the hidden time 9 stamp that you theorize is within the Blackberry message ID, 10 that hidden time stamp, if there was any error or malfunction 11 in the clock of a particular device would be affected 12 theoretically, right? 13 A. Yes. 14 Q. And you have observed, haven't you, that there are 15 sometimes errors within the clocks of different computer 16 devices, right? 17 A. That's correct. 18 Q. It's also possible that, for example, if a message were 19 sent -- composed, and for whatever reason didn't actually get 20 sent for some time, if it was stuck in an inbox, that it could 21 end up having a different time stamp on it than the time of a 22 composed -- that the email was composed, correct? 23 A. That's correct, with the caveat it would always be in the 24 future. 25 Q. Right. So, for example, exactly, with the caveat it would	1 this particular email was never created, right? 2 THE COURT: I don't understand the question. I'm 3 sorry, you mean wasn't created at the time that it purportedly 4 was created? 5 MR. JACKSON: Yes, your Honor. 6 THE WITNESS: It's so far outside the realm of 7 possibility that that is why I say definitively this is a fake 8 email. Because it's hard to conceive of even a scenario where 9 for some reason it would deviate from standard hex as found in 10 the well-known format of a UUID. 11 Q. And can you explain to us where you got your training on 12 UUIDs? 13 A. So initially I think it was when I was learning about 14 databases, and I never really transferred it into emails, but 15 it was learning about databases in part of my computer science 16 training that began around 2014. 17 THE COURT: And are you saying that you learned about 18 the UUID as part of that training? 19 THE WITNESS: Yes. 20 THE COURT: And one of the things you learned was the 21 whole A to F letters? 22 THE WITNESS: Yes. 23 THE COURT: And there's never any letters but A 24 through F? 25 THE WITNESS: A UUID is a hexadecimal representation.				

HCITTUZ7	DeCapua - Redirect	Page 6335	HCITTUZ7	Page 6337
1	THE COURT: Now in the work that you have done since		1	embark on this presentation of evidence. The witness order was
2	2014, have you encountered this UUID in the investigations you		2	going to be Special Agent Amato, Special Agent DeCapua, and
3	have been involved in?		3	then Mr. Maiden.
4	THE WITNESS: I have encountered it. Sometimes it's		4	THE COURT: Well, I'm sort of wondering, Mr. Jackson
5	used to designate a specific device, a device will have its own		5	may have other questions he wants to ask, and I'm kind of
6	UUID, or another term is GUID.		6	wondering when that's going to happen. I guess if you reach a
7	THE COURT: GUID?		7	point where you have gotten to the point in your proof where
8	THE WITNESS: GUID. They mean the same thing. I have		8	you want to call Agent DeCapua, we'll have to take a break to
9	never delved into it as deeply as I have today, but I have come		9	allow Mr. Jackson to conduct further examination and see where
10	across it.		10	that heads.
11	THE COURT: And you have seen these -- I take it in		11	But I will say, based on what I heard so far, subject
12	other message IDs you have seen these UUIDs.		12	to whatever Mr. Jackson comes up, that the nature of Agent
13	THE WITNESS: I have, and it's always hex.		13	DeCapua's testimony tonight addresses a number of the problems
14	MR. JACKSON: Your Honor, at this time I would like to		14	I raised with you earlier today in that, subject of course to
15	ask for some time to evaluate. This is a lot of scientific		15	argument and further examination by Mr. Jackson, it does appear
16	information. I would like to ask for some time to evaluate		16	to me that the agent has sufficient experience and training
17	this testimony.		17	with respect to issues he testified about tonight that it would
18	THE COURT: Yes. Yes.		18	be appropriate to have him testify in the way he did tonight
19	Ms. Griswold, anything else that you want to ask at		19	about a message IDs and their contents.
20	this point?		20	The agent has expressed an opinion, unlike the
21	MS. GRISWOLD: Could I ask one more question?		21	testimony at the prior hearing, he's explained the basis for
22	THE COURT: Sure.		22	his opinion, and more than that I really can't say. But I do
23	REDIRECT EXAMINATION		23	feel you have addressed the problems I raised with you, in
24	BY MS. GRISWOLD:		24	particular, I gather from your earlier comments you do not
25	Q. Special Agent DeCapua, once you found the hidden time stamp		25	intend to go back to the idea of trying to demonstrate that a
HCITTUZ7		Page 6336	HCITTUZ7	Page 6338
1	you were asked some questions about whether or not you had		1	fabricated email was placed back into Yahoo. We're not going
2	been -- had cases before where there was a hidden time stamp,		2	to see a demonstration along those lines.
3	but once you found it and you found the epoch time stamp, that		3	MS. GRISWOLD: That's correct. My present intention
4	feature is how common, an epoch time stamp?		4	would be, with the Court's permission, to introduce Government
5	A. It's very common.		5	Exhibit 2908, the communication between Mr. Amanat and his
6	Q. So your analysis of the epoch time stamp, once you found		6	brother, to have the special agent demonstrate how emails could
7	it, was that a familiar analysis to you?		7	be pulled down, then after having laid a foundation and having
8	A. Yeah, I instantly recognized it. And I convert epoch time		8	him qualified, ask him if he could offer an opinion based only
9	stamps to human readable time stamps all the time.		9	on the fact an email appears in the Yahoo account whether that
10	MS. GRISWOLD: Nothing further at this time, your		10	email is authentic, and then move onto -- if we need to take a
11	Honor.		11	break, that would be the time, and we would, if allowed, then
12	THE COURT: All right. You can step down.		12	pivot to the testimony about the message ID in those three
13	So I know, Mr. Jackson, you want some time to digest		13	emails.
14	what you heard. I'm sort of wondering what is going to happen		14	I should note we have the Yahoo witness. I had been
15	tomorrow. So I know there's a few documents that are going to		15	discussing with Mr. Jackson. She lives in California and she
16	be introduced, but after that it's not really clear to me what		16	has a young child and her daycare is closed this week. So we
17	is going to happen, and I'm a little worried about what we're		17	have been discussing a stipulation as to her testimony, and I
18	going to do with the jury.		18	believe we had -- almost had agreement on that.
19	What are your intentions tomorrow, assuming the		19	THE COURT: Is that true, Mr. Jackson?
20	defense rests early?		20	MR. JACKSON: That's correct, your Honor, basically we
21	MS. GRISWOLD: We would like to go into this		21	have agreed on a stipulation.
22	fabrication evidence. My first witness was going to be Special		22	THE COURT: All right. Let me just look at my notes
23	Agent Amato to talk about her review of Mr. Maiden's computer.		23	and see if I have any questions before you leave.
24	I would obviously like to know whether or not I would be able		24	MR. NAFTALIS: One issue, and we could talk to
25	to offer the testimony of Special Agent DeCapua before we		25	Mr. Jackson, we intended to call his paralegal. We're trying

**In The Matter Of:**  
*UNITED STATES OF AMERICA, V*  
*KALEIL ISAZA TUZMAN, et al.,*

---

*December 20, 2017*

---

*Southern District Court Reporters*

Original File HckWtuzF.txt  
Min-U-Script® with Word Index

HckWtuz2	Amato - Redirect	Page 6537	HckWtuz2	DeCapua - Direct	Page 6539
1	Q. Does the gap on Mr. Maiden's computer cover any of the		1	(In open court)	
2	dates that are listed on Amanat Exhibits 9002, 908, 9010 and		2	JOEL DECAPUA,	
3	913 --9013?		3	called as a witness by the Government,	
4	THE COURT: 9013, right?		4	having been duly sworn, testified as follows:	
5	MS. GRISWOLD: 9013. Thank you, your Honor.		5	THE COURT: Please proceed.	
6	A. So, for Amanat Exhibit 908, emails appear began appearing		6	MS. GRISWOLD: Thank you, your Honor.	
7	again in Mr. Maiden's account on March 10, 2009.		7	DIRECT EXAMINATION	
8	Q. So there are emails --		8	BY MS. GRISWOLD:	
9	A. There are emails for March 10, 2009.		9	Q. Good morning.	
10	Q. Are there emails for December 2, 2008?		10	A. Good morning.	
11	A. Yes.		11	Q. Where do you work?	
12	Q. Are there emails for June 2, 2011?		12	A. I work at the Federal Bureau of Investigation.	
13	A. Yes.		13	Q. What is your position there?	
14	Q. Are there emails for March 26, 2012?		14	A. I'm a special agent.	
15	A. Yes.		15	Q. What squad are you assigned to?	
16	MS. GRISWOLD: No further questions.		16	A. I'm assigned to cyber crimes task force on squad CY-2.	
17	THE COURT: Anything else, Mr. Jackson?		17	Q. How long have you been on the cyber crimes task force?	
18	MR. JACKSON: No. Thank you, your Honor.		18	A. I first joined in 2014.	
19	THE COURT: You can step down, Agent.		19	Q. How long have you been with the FBI in total?	
20	(Witness excused)		20	A. Since 2009, so I believe it's nine years.	
21	THE COURT: The government will call its next witness.		21	Q. Between 2009 and 2014, what type of squad were you assigned	
22	MS. GRISWOLD: The government calls Special Agent Joel		22	to?	
23	DeCapua.		23	A. Prior to the cyber crimes squad, I was assigned to a squad	
24	MR. WEITZMAN: Your Honor, may we approach?		24	focused on securities fraud and public corruption.	
25	THE COURT: Yes. (Continued on next page)		25	Q. Did those cases involve the review of emails?	
HckWtuz2	Amato - Redirect	Page 6538	HckWtuz2	DeCapua - Direct	Page 6540
1	(At sidebar)		1	A. Yes, they did.	
2	MR. WEITZMAN: I just want to put on the record my		2	Q. Turning back to the cyber squad, what types of cases does	
3	client isn't feeling so well today, Judge. He has an upset		3	your squad investigate?	
4	stomach, and he'll be in and out of the courtroom at times. We		4	A. Generally we investigate any type of hacking case or cyber	
5	waive his presence during the times he's out of the courtroom.		5	crime case that has any criminal nexus as opposed to a national	
6	THE COURT: Thank you, Mr. Weitzman.		6	security nexus.	
7	MR. WEITZMAN: You're welcome.		7	Q. Have your cases while on the cyber squad involved the	
8	(Continued on next page)		8	execution of email search warrants?	
9			9	A. Yes.	
10			10	Q. Have your cases involved the examination of computers for	
11			11	email content?	
12			12	A. Yes.	
13			13	Q. I want to turn to some of the training that you've	
14			14	undertaken at the FBI in the area of electronic or digital	
15			15	evidence. When new agents join the FBI, is there any training	
16			16	in digital forensics?	
17			17	A. There is. At Quantico, we are given new-agents training,	
18			18	which includes training on how to review email headers, how to	
19			19	investigate crimes involving the Internet and generally how to	
20			20	go about gathering digital evidence and then analyzing it for	
21			21	review.	
22			22	Q. Before we turn to additional training, you just used the	
23			23	term "email headers." Can you describe for the jury what you	
24			24	mean by that term?	
25			25	A. Sure. So, I've learned that emails are -- they're made up	

UNITED STATES OF AMERICA, V  
KALEIL ISAZA TUZMAN, et al.,

December 20, 2017

HckWtuz2	DeCapua - Direct	Page 6541	HckWtuz2	DeCapua - Direct	Page 6543
1	of two parts. The first part is the content, which is what you		1	digital forensics.	
2	would see on the screen, the words or the links or whatever is		2	Q. Is GIAC a place that is used by FBI cyber agents to obtain	
3	in the email, and the other part is the header, which is mostly		3	certifications and training?	
4	invisible to someone who sends or receives an email, but if you		4	A. Yeah, that's correct.	
5	know where to look, you can, you can find the header and you		5	Q. Which of these certifications is relevant to the analysis	
6	can analyze it, and it's useful to us because it has good		6	of emails and email headers?	
7	forensic artifacts that we can study.		7	A. So, of these certifications, I think the first one that's	
8	Q. Once you became a cyber agent in 2014, did you receive		8	relevant is the March 2008 certified fraud examiner. You learn	
9	additional training in the area of digital forensics?		9	some things about digital forensics and analyzing emails, in	
10	A. I did.		10	that course of certification. I'm no longer certified; I've	
11	Q. Can you describe that training, please?		11	let it lapse.	
12	A. So, there was on-the-job, sponsored by the FBI, digital		12	The March 2015 certification, the GSEC, is another course	
13	forensics training. Some of it was self-study. Some of it		13	of study I took where we learned about digital forensics, and	
14	was, I would go on the Internet and go through a course of		14	there's a part in that course of study that involves the	
15	study. Some of it was in person. Most of it was through a		15	analysis of emails and email headers. It culminates in a	
16	private company called SANS. At SANS I took a lot of training		16	five-hour test that I took and passed, and that's why I	
17	to include a lot about how to analyze email headers and digital		17	received this certification.	
18	forensics, and I was tested on that training. I received		18	July 2015 certification, certified forensic examiner, is	
19	certifications on it.		19	a -- is another course of study, and then a, a certification	
20	MS. GRISWOLD: If we could please pull up for the		20	test that I took that involved analysis of digital evidence and	
21	witness, counsel and the Court what is marked as Government		21	email headers.	
22	Exhibit 3584.		22	The next one would be October 2016 course, the certified	
23	Would you like another copy, your Honor?		23	forensic analyst, which is another course of study that goes	
24	THE COURT: I have it. Thank you.		24	through how to analyze email headers and how to handle digital	
25	BY MS. GRISWOLD:		25	evidence, and I took a certification course and I'm certified	
HckWtuz2	DeCapua - Direct	Page 6542	HckWtuz2	DeCapua - Direct	Page 6544
1	Q. Do you recognize Government Exhibit 3584, Special Agent		1	in it.	
2	DeCapua?		2	The March 2017, the network forensic analyst, is another	
3	A. I do.		3	that handles additional topics in how to analyze email headers.	
4	Q. How do you recognize it?		4	And the March 2017 course, the FBI-sponsored digital extraction	
5	A. It is a résumé I created.		5	technician training, it is another that -- it's a two-week	
6	MS. GRISWOLD: The government offers Government		6	course with, culminating in a test and which I took and passed,	
7	Exhibit 3584.		7	which is about the extraction of digital evidence and the	
8	THE COURT: Any objection?		8	analysis and review afterward.	
9	MR. JACKSON: No objection.		9	Q. In total, approximately how many email headers have you	
10	MR. WEITZMAN: No objection.		10	reviewed in your career?	
11	THE COURT: 3584 is received.		11	A. Hundreds.	
12	(Government Exhibit 3584 received in evidence)		12	MS. GRISWOLD: You can take that down, please.	
13	MS. GRISWOLD: Permission to publish?		13	Q. Are you familiar with the term "web mail"?	
14	THE COURT: Yes.		14	A. I am.	
15	BY MS. GRISWOLD:		15	Q. What is it?	
16	Q. Is this a résumé, your résumé?		16	A. Web mail is a service like GMail or HotMail or Yahoo Mail,	
17	A. Yes.		17	that allows you to send and receive emails using their email	
18	Q. And it has three sections: career summary; certifications,		18	servers. You log in and you create an account and you can use	
19	training and professional affiliations; and finally, education?		19	it to send and receive emails.	
20	A. That's correct.		20	Q. Are you familiar with the term "local email client"?	
21	Q. I want to focus on the middle section, certifications,		21	A. I am.	
22	training and professional affiliations. Can you identify which		22	Q. What does that term mean?	
23	of these certifications -- first of all, what is GIAC that		23	A. A local email client is a piece of software that you have	
24	appears in a number of places here?		24	on your computer or your phone, even, such as Outlook or Apple	
25	A. GIAC is an entity that tests and certifies practitioners of		25	Mail or Thunderbird, that allows you, from your personal	

HckWtuz2	DeCapua - Direct	Page 6545	HckWtuz2	DeCapua - Direct	Page 6547
1	computer, to interact with one of the web mail services so you		1	Yahoo site but download them onto my laptop. How can I do	
2	can type up emails on your home computer and click send in		2	this? I'm concerned about them subpoenaing Yahoo at some	
3	Outlook and it will automatically reach out to the, to the web		3	point."	
4	mail service and make sure everything is synced and sent and		4	MS. GRISWOLD: If we could please go to Irfan Amanat's	
5	received properly.		5	response at 2321.	
6	Q. Are you familiar with any protocols that allow local email		6	Q. If you could please read the response.	
7	clients, such as Outlook or Apple Mail, to communicate with a		7	A. "Set up your Outlook to pull all your emails from Yahoo and	
8	web mail account, such as Yahoo?		8	delete it. If you need help, I can walk you through it."	
9	A. Yeah, there's several protocols that are used. The most		9	Q. Based on your training and experience as an FBI agent and	
10	familiar is the IMAP protocol.		10	on dealing with email evidence, are you familiar with how to	
11	Q. Is that I-M-A-P?		11	pull emails from a web mail account such as Yahoo, onto a local	
12	A. Yes.		12	client account such as Outlook?	
13	Q. Can you describe that?		13	A. I am.	
14	A. So, it stands for the Internet message access protocol, and		14	Q. Do you need any special FBI or proprietary software to do	
15	it's just an agreed upon -- a protocol is an agreed-upon		15	this?	
16	language that two computers or two servers will use to		16	A. No.	
17	communicate with each other and exchange information. And		17	MS. GRISWOLD: At this time, your Honor, we would ask	
18	specifically IMAP is used for the communications between an		18	that Special Agent DeCapua be allowed to hook up his laptop so	
19	email server such as the one that Google would have or		19	he can provide a brief demonstration to the jury.	
20	something that your employer might have and the local email		20	THE COURT: Yes.	
21	client, such as Outlook.		21	Q. In preparation for your testimony, did you create a web	
22	Q. Are you familiar with the term "spoofing"?		22	mail account on Yahoo to use for a demonstration?	
23	A. I am.		23	A. I -- yes, I did.	
24	Q. What is it?		24	Q. Is jamessmith53490@yahoo.com the account you created?	
25	A. Spoofing generally refers to, in the context of emails,		25	A. It is.	
HckWtuz2	DeCapua - Direct	Page 6546	HckWtuz2	DeCapua - Direct	Page 6548
1	when someone is forging an email. Either they're making it		1	Q. And to create this account, did you go to yahoo.com?	
2	seem like it's coming from someone who never sent it or they're		2	A. I did.	
3	changing the date or changing the content or changing some		3	Q. If you could keep your voice up as well. Thank you.	
4	other aspect of the email in order to make it fraudulent.		4	Let's pull up yahoo.com on your computer.	
5	Q. And do you have training at the FBI on spoofing?		5	So we're at yahoo.com. Can you go ahead and log in to the	
6	A. I do.		6	James Smith account that you created?	
7	Q. Does that involve the review of email headers?		7	A. Certainly. So I logged into it previously so it	
8	A. It does.		8	automatically saved my password and user name, and it just	
9	MS. GRISWOLD: Your Honor, may Special Agent DeCapua		9	opened up into the web mail access point for the James Smith	
10	offer an opinion related to the analysis of electronic		10	account.	
11	evidence, including email headers and email platforms?		11	Q. Did you receive an email from the government in preparation	
12	THE COURT: Any objection?		12	for your demonstration today?	
13	MR. JACKSON: No, your Honor.		13	A. I did.	
14	THE COURT: Yes, he may offer opinion testimony on		14	Q. Is that email in your inbox for this account?	
15	those subjects.		15	A. Yes, it is.	
16	MS. GRISWOLD: Thank you, your Honor.		16	Q. Can you open that up? Is this the email from Mr. Naftalis	
17	MR. JACKSON: Your Honor, just to be clear, as we		17	on December 18 at 8:58 p.m.?	
18	previously discussed.		18	A. It is.	
19	THE COURT: Yes.		19	Q. And the content of that email says, "Hi, Joel"?	
20	MS. GRISWOLD: I'd like to show the witness what is in		20	A. That's correct.	
21	evidence as Government Exhibit 2908, please.		21	Q. Can you tell the jury where you find the header information	
22	Q. If you could direct your attention to the June 14, 2008,		22	for this email?	
23	email at 2205. If you could read that, please, Special Agent		23	A. So, every service is different. On Yahoo you have to go to	
24	DeCapua. It's an email from Omar Amanat to Irfan Amanat.		24	"more" and then "view raw message."	
25	A. "Hey Iffi, I also want to delete all of my emails from the		25	Q. What are we looking at now?	

UNITED STATES OF AMERICA, V  
KALEIL ISAZA TUZMAN, et al.,

December 20, 2017

HckWtuz2	DeCapua - Direct	Page 6549	HckWtuz2	DeCapua - Direct	Page 6551
<p>1 A. So as I testified before, an email is made up of two parts, 2 the content and then the header. Right here, you see all this 3 seemingly random numbers and dates. This is all part of the 4 header. It isn't until you get down to the very bottom that 5 you see the actual content, which is just the words "Hi, Joel." 6 And, of course, however long the content is and whether there's 7 links or anything else, it will be included after the header 8 information.</p> <p>9 MS. GRISWOLD: And the Message-ID that's in the 10 middle, can we highlight that. Scroll down a little.</p> <p>11 Q. Do you see that?</p> <p>12 A. I do.</p> <p>13 Q. Are you familiar with the term "Message-ID"?</p> <p>14 A. I am.</p> <p>15 Q. What is it?</p> <p>16 A. So, as I said before, as a, as a forensicator, there's 17 certain things in a message header that we find has value as 18 digital artifacts, and one of those things in particular is 19 something called a Message-ID. Now, a Message-ID is completely 20 invisible to you when you send or receive an email unless you 21 go in and view the raw message, but the Message-ID is -- it's a 22 unique number that is assigned to every single email that's 23 sent, and it -- there's certain characteristics of it that we 24 can analyze and we can make certain conclusions about the 25 underlying email.</p>	<p>1 Q. Can you show the jury how you're able to pull this email 2 from the Yahoo account onto your local email client?</p> <p>3 A. Absolutely.</p> <p>4 Q. And if you could just narrate the steps that you're taking 5 when you're doing it.</p> <p>6 A. So the first thing I do, and you may recognize this 7 program, is just open up the mail program, and because I've 8 never set it up before, it's going to ask me for my user name 9 and password. When I hit create, it's reaching out to Yahoo's 10 server and it's authenticating that my password is correct, and 11 then it's going to prompt me with an option to set up the 12 account, and when I do, the local email client is going to 13 reach out to the server hosted by Yahoo. They're going to 14 communicate over the IMAP protocol, and they're going to sync. 15 And what that means is the local email client is going to look 16 at Yahoo's server and say, Is there anything here that's not on 17 the local email client? And it's going to find the email 18 message that Mr. Naftalis sent me and it's going to pull that 19 down onto my local email client, so I push "create."</p> <p>20 Q. And the inbox that we're looking at now, is that from your 21 Apple Mail?</p> <p>22 A. Yes, it is. And so here, you see it took a few seconds, 23 but it pulled down the email that was stored on Yahoo's server.</p> <p>24 Q. Can you open that email up?</p> <p>25 Now, can you pull this email onto your laptop and save</p>				
HckWtuz2	DeCapua - Direct	Page 6550	HckWtuz2	DeCapua - Direct	Page 6552
<p>1 Q. You just used the term "forensicator." What does that term 2 mean?</p> <p>3 A. A forensicator is something that is used colloquially 4 within the digital forensics community just to refer to someone 5 who practices digital forensics.</p> <p>6 THE COURT: You've also used the term "digital 7 artifact." Could you tell us what you mean when you say 8 digital artifact.</p> <p>9 THE WITNESS: Absolutely. So an artifact just means 10 something that we find that can give us some insight on what 11 happened in the past. If you're Indiana Jones, you're looking 12 at sarcophaguses and writings on walls. For us, we're looking 13 for things like time stamps or any other pieces of data that 14 can tell us what happened in the past.</p> <p>15 THE COURT: With respect to an email message.</p> <p>16 THE WITNESS: That's correct. We use the term 17 generally throughout digital forensics, but in respect to an 18 email header and message, there's also forensics -- there's 19 also digital artifacts within a header.</p> <p>20 THE COURT: OK.</p> <p>21 BY MS. GRISWOLD:</p> <p>22 Q. Do you have a local email client on your laptop?</p> <p>23 A. I do.</p> <p>24 Q. What do you have?</p> <p>25 A. I have Apple Mail.</p>	<p>1 it onto your laptop?</p> <p>2 A. Yes.</p> <p>3 Q. Can you walk the jury through how you do that and narrate 4 as you just did?</p> <p>5 A. Sure. So the easiest way, it is technically on my laptop 6 right now, but in order to save it on my laptop and a place 7 that I know how to quickly get to it, I would just export my 8 mailbox. And to do that I would go to "mailbox," "export 9 mailbox." It will ask me where I want to put it. I'm just 10 going to say on the desktop, and you'll see there's a new file 11 here called inbox.mbox, and that's where the emails are stored.</p> <p>12 Q. Can you open up the email you just saved on your desktop?</p> <p>13 A. Sure.</p> <p>14 MR. JACKSON: Objection, your Honor.</p> <p>15 THE COURT: Grounds.</p> <p>16 MR. JACKSON: Scope. Discussion yesterday.</p> <p>17 THE COURT: All right. I'll hear you at sidebar.</p> <p>18 (Continued on next page)</p> <p>19</p> <p>20</p> <p>21</p> <p>22</p> <p>23</p> <p>24</p> <p>25</p>				

HckWtuz2	DeCapua - Direct	Page 6553	HckWtuz2	DeCapua - Direct	Page 6555
1	(At sidebar)		1	(In open court)	
2	THE COURT: All he's done so far is he's brought it		2	BY MS. GRISWOLD:	
3	down from the Yahoo server. He's stored it on the desktop of		3	Q. Now that you have the email saved on your desktop, can I	
4	his laptop, and she's asked him whether he can open up the		4	ask you to close out of that file and go back to Yahoo and show	
5	email. I didn't see that as implicating any of our discussion		5	the jury how you can delete the email from both Yahoo and your	
6	yesterday. Are you troubled by anything that's happened so		6	local email client?	
7	far?		7	A. So now I'm back to Yahoo. And there's just the one email,	
8	MR. JACKSON: Your Honor, I'm just a little bit		8	so I just click it and go to delete. And then I would just	
9	concerned about what the next step is.		9	empty my trash. And in doing so, the email no longer exists at	
10	THE COURT: OK. So you want to know what's happening		10	Yahoo. The only place the email exists right now is on my	
11	next.		11	laptop computer.	
12	MR. JACKSON: I want to know what's happening next		12	Q. Did you use any FBI or proprietary software to do the	
13	because it's not clear to me why we need to take the last step.		13	demonstration that you just provided?	
14	MS. GRISWOLD: The steps that we took, our view is		14	A. No. This is all stuff just out of the box.	
15	that's exactly consistent with what Government Exhibit 2908		15	Q. What do you mean when you say out of the box?	
16	says. It says pull from Yahoo onto Outlook and onto my laptop.		16	A. It comes preloaded on the computer.	
17	He's now shown it exists on his laptop. Now we're just going		17	Q. Based on your experience as an FBI agent and obtaining	
18	to delete it from Yahoo. I'm not going to at this point say,		18	search warrants, email search warrants, if you were to obtain	
19	Can you alter it, or anything like that.		19	an email search warrant for all email content in this James	
20	When we get to the later testimony, he's going to		20	Smith account at this moment, what would you expect to receive	
21	testify about the specific features of the emails that he		21	in response?	
22	looked at that were produced by the defendant, but at this		22	A. I would --	
23	point, I'm not intending to do anything else with this, messing		23	MR. JACKSON: Objection.	
24	with this email.		24	THE COURT: Do you want to approach on this?	
25	MR. JACKSON: OK. Thank you. I appreciate that. The		25	MR. JACKSON: Yes, your Honor.	
HckWtuz2	DeCapua - Direct	Page 6554	HckWtuz2	DeCapua - Direct	Page 6556
1	one thing I will say, your Honor, is that going back to Yahoo		1	THE COURT: OK.	
2	and deleting the email was not part of what the government's		2	(Continued on next page)	
3	proffer was as to what the demonstration would be yesterday. I		3		
4	think this is the end of what they proffered to demonstrate,		4		
5	their efforts to go back to the email in Yahoo and delete.		5		
6	Now I understand there's an email where my client		6		
7	discusses it, but I think it's much more speculative testimony		7		
8	in terms of the demonstration. We're no longer demonstrating a		8		
9	function that is a contested function that they can connect,		9		
10	something that theoretically could have happened. We're now		10		
11	going into something that's beyond the scope of their proffer,		11		
12	and I don't think it's necessary. I think you can ask Special		12		
13	Agent DeCapua, Can you delete the email from Yahoo without		13		
14	doing a demonstration of that, and I wouldn't object to that.		14		
15	MS. GRISWOLD: I disagree. We've tried to be very		15		
16	careful, but the email says delete the messages from Yahoo.		16		
17	THE COURT: I agree.		17		
18	(Continued on next page)		18		
19			19		
20			20		
21			21		
22			22		
23			23		
24			24		
25			25		

UNITED STATES OF AMERICA, V  
KALEIL ISAZA TUZMAN, et al.,

December 20, 2017

HckWtuz2	DeCapua - Direct	Page 6557	HckWtuz2	DeCapua - Direct	Page 6559
1	(At sidebar)		1	(In open court)	
2	THE COURT: The point is that the email no longer		2	BY MS. GRISWOLD:	
3	exists on the email server.		3	Q. So the Yahoo account at this point has no emails in it,	
4	Is that your point?		4	correct?	
5	MS. GRISWOLD: Yes.		5	A. Correct.	
6	THE COURT: And you object.		6	Q. In the James Smith account?	
7	MR. JACKSON: Yes, your Honor. I don't think the		7	A. Correct.	
8	witness has a foundation for that, and I think it's factually		8	MS. GRISWOLD: OK. We can close out of the	
9	incorrect. In fact, I think it's widely advertised by most of		9	demonstration. Thank you.	
10	the web mail services that you can delete your account and		10	Q. Now, the process that you just demonstrated, does it work	
11	recover it with some --		11	the other way; that is, can you take the email on your laptop	
12	MS. GRISWOLD: But at this moment --		12	and put it back into the Yahoo account using the method that	
13	I'll let you finish your thought.		13	you just demonstrated?	
14	MR. JACKSON: The question was, What would you expect		14	A. Yes, you can.	
15	to recover if you issued a search warrant? I don't think that		15	Q. Based on your experience, the way that a web mail account	
16	this witness could testify that if a warrant was issued to		16	and the local email client account interact, are you able to	
17	Yahoo it would be able to get the content we just saw. If it		17	offer an opinion on whether the fact that an email exists in a	
18	was recoverable, then certainly it's conceivable to me that		18	web mail account means the email is authentic?	
19	Yahoo --		19	MR. JACKSON: Objection. Vague.	
20	MS. GRISWOLD: I don't think that that would be his		20	THE COURT: All right. I'll hear you at sidebar.	
21	testimony. The only place that that email exists now is on his		21	(Continued on next page)	
22	laptop. Yahoo would only have what's on their servers, and		22		
23	there's nothing on that server right now.		23		
24	MR. JACKSON: This witness does not have sufficient --		24		
25	THE COURT: I tend to agree that there is no		25		
HckWtuz2	DeCapua - Direct	Page 6558	HckWtuz2	DeCapua - Direct	Page 6560
1	foundation at this point for him to testify about what would be		1	(At sidebar)	
2	produced in response to a search warrant if Yahoo got one now		2	THE COURT: I thought we covered this yesterday. I	
3	for the James Smith account.		3	thought you were OK with this question, but it appears that	
4	MS. GRISWOLD: OK. I'll move on.		4	you're not.	
5	(Continued on next page)		5	MR. JACKSON: No, your Honor. You're right, I'm OK	
6			6	with this concept. My problem is the language of the question.	
7			7	THE COURT: OK.	
8			8	MR. JACKSON: Does it mean that the email is	
9			9	authentic, I don't know what that means in the context of that	
10			10	question. When you talk about all the "if there's an email	
11			11	that is in an account, it's an authentic something," OK, so I	
12			12	just think that the question leaves a great degree of	
13			13	ambiguity, and it's very difficult for me to interrogate.	
14			14	MS. GRISWOLD: Then I can ask him whether or not prior	
15			15	to putting it back up on the Yahoo account it's possible to	
16			16	make changes. I don't have to link it to the specific emails	
17			17	at issue here, if that's your concern; then that would be the	
18			18	natural question to ask.	
19			19	MR. JACKSON: I think that we already went over the	
20			20	fact that I don't think this witness has sufficient, I don't	
21			21	think this witness has sufficient basis to offer that specific	
22			22	opinion, but I think the question -- this is just my	
23			23	suggestion. I think the question that should be asked is, Does	
24			24	the fact that an email is in a Yahoo account mean that the	
25			25	email was necessarily sent when the email purports to have been	

UNITED STATES OF AMERICA, V  
KALEIL ISAZA TUZMAN, et al.,

December 20, 2017

HckWtuz2	DeCapua - Direct	Page 6561	HckWtuz2	DeCapua - Direct	Page 6563
1	sent.		1	there that people know," and the remaining part of the answer	
2	THE COURT: Or you could ask something like, Can you		2	is struck from the record, and the jury should disregard it.	
3	conclude from the presence of an email on the Yahoo web mail		3	BY MS. GRISWOLD:	
4	service that it accurately reflects content, date sent?		4	Q. Special Agent DeCapua, when an individual has control over	
5	MR. JACKSON: I think the judge's question is the best		5	their own web mail account, such as the control that you have	
6	question.		6	with the James Smith account, do they have access to the header	
7	MS. GRISWOLD: And then I'm going to say why not, and		7	information of the email?	
8	he's going to say because if you have control of the account,		8	A. They do.	
9	you can make alterations to it. That was the testimony at the		9	Q. And are they able to alter the information in that	
10	hearing as well. I just want to be clear so we don't come back		10	header --	
11	for another sidebar. So the clear question that the Court		11	A. Yes, they --	
12	thinks is most appropriate would be to ask whether or not based		12	Q. -- if they have control over the account?	
13	on the email in the Yahoo account you can tell whether or not		13	A. Yes, they are.	
14	the person who is sending, the time, the details in it are, in		14	Q. Are they able to alter the content if they have access to	
15	fact, authentic.		15	the account?	
16	MR. JACKSON: It's the word "authentic." What the		16	A. Yes, they are.	
17	Court said was whether you can tell whether that information --		17	Q. Now I want to turn to some of the specific emails in	
18	THE COURT: Maybe we should write it down.		18	evidence in this case. Let me ask you to define a few terms.	
19	MS. GRISWOLD: I apologize, your Honor.		19	You talked about the Message-ID before. Are you familiar with	
20	THE COURT: I'll get a piece of paper. My question		20	the term "epoch," E-P-O-C-H?	
21	started with, Can you conclude from the presence of an email on		21	A. Yes, I am.	
22	a web mail service such as Yahoo that it accurately reflects		22	(Continued on next page)	
23	the date it was sent, the content of the email and the sender		23		
24	and recipient?		24		
25	MR. JACKSON: Thank you,. (Continued on next page)		25		
HckWtuz2	DeCapua - Direct	Page 6562	HCKTTUZ3	DeCapua - Direct	Page 6564
1	(In open court)		1	BY MS. GRISWOLD:	
2	BY MS. GRISWOLD:		2	Q. What does it mean?	
3	Q. Special Agent DeCapua, can you conclude from the presence		3	A. So an epoch time stamp is a way of telling time and date.	
4	of an email in a Yahoo account, on the Yahoo servers, that the		4	We use the Julian calendar, March 15, 2009. Computers use	
5	email in that account accurately reflects the date it was sent?		5	something that is easier for them to understand, and the most	
6	A. Absolutely not.		6	commonly used way for computers to tell the time and date is	
7	Q. Can you conclude from the presence of the email in a Yahoo		7	something called an epoch timestamp, which all it is is the	
8	account that it accurately reflects the content of the email?		8	number of seconds that have a passed since midnight	
9	A. You cannot.		9	January 1st, 1970 in Greenwich Mean Time, and it's a number in	
10	Q. Can you conclude from the presence of the email in the		10	the billions right now, and most forensic timestamps we see are	
11	Yahoo account that it accurately reflects the sender or		11	in epoch timestamp format.	
12	recipient?		12	THE COURT: You just mentioned Greenwich Mean Time.	
13	A. You cannot.		13	What is Greenwich Mean Time?	
14	Q. Why not? And keep your voice up?		14	THE WITNESS: Greenwich Mean Time is the time zone	
15	A. The reason is an email is not self-authenticating, so if it		15	that London, England is in.	
16	appears in one place, that doesn't mean anything because it can		16	BY MS. GRISWOLD:	
17	be spoofed and put there using a technique that is out there		17	Q. How frequently have you come across epoch timestamps in the	
18	that people know how to do, and it involves using the IMAP --		18	course of your review of email headers?	
19	MR. JACKSON: Objection, your Honor.		19	A. This would be the first time that I have looked at an epoch	
20	THE COURT: Sustained. Sustained.		20	timestamp in a email header, but in my review of digit	
21	MR. JACKSON: Move to strike the last answer.		21	evidence, it's all the time.	
22	THE COURT: The entire last answer?		22	Q. And when you say "all the time," can you give us an example	
23	MR. JACKSON: No, your Honor. Just the last part,		23	of where you have come across an epoch timestamp?	
24	from "out there."		24	A. You find it in network logs mostly. When someone tells us	
25	THE COURT: Yes. The answer from the point of "out		25	they were hacked and we ask for the network logs and we're	

UNITED STATES OF AMERICA, V  
KALEIL ISAZA TUZMAN, et al.,

December 20, 2017

HCKTTUZ3	DeCapua - Direct	Page 6565	HCKTTUZ3	DeCapua - Direct	Page 6567
1	trying to figure out when dates and times that things happened,		1	the underlying emails with header information related to Amanat	
2	most of it will be in an epoch timestamp, and I would have do		2	Exhibits 908, 9010 and 9013 to the government.	
3	the conversion from epoch to something that I can understand.		3	Paragraph five. Government Exhibits 3550, 3551, and	
4	Q. Two more terms before we turn to some emails. Are you		4	3552 are copies of the underlying emails with header	
5	familiar with the format UUID?		5	information related to Amanat Exhibits 908, 9010 and 9013.	
6	A. I am.		6	At this time the government would offer Government	
7	Q. What does it stand for and what does it mean?		7	Exhibits 3550, 3551 and 3552.	
8	A. UUID stands for Universal Unique Identifier. And what it		8	MR. JACKSON: No objection.	
9	is something that is very commonly used in computing. And		9	THE COURT: 3550, 3551 and 3552 are received in	
10	it's just a number, it's like a serial number, but it has a		10	evidence.	
11	very specific format that when you look at it, you recognize		11	(Government's Exhibits 3550, 3551 and 3552 received in	
12	it.		12	evidence)	
13	Q. Have you had training in computer science?		13	BY MS. GRISWOLD:	
14	A. I have.		14	Q. You have those documents in front of you, Special Agent	
15	Q. Are you familiar with the term hexadecimal?		15	DeCapua?	
16	A. I am.		16	A. I do.	
17	Q. Can you spell that for the court reporter?		17	Q. Let's start with Government Exhibit 3550.	
18	A. Hexadecimal is spelled H-E-X-I-D-E-C-I-M-A-L.		18	MS. GRISWOLD: Permission to publish that, your Honor?	
19	Q. And what does hexadecimal mean?		19	THE COURT: Yes.	
20	A. So our counting system has base ten, we count one through		20	MS. GRISWOLD: And can we please put this up side by	
21	ten. For computers, because of the way they're built and how		21	side with Amanat Exhibit 908, which is in evidence, in redacted	
22	they work, it's easier for them to count using a base 16.		22	form.	
23	Hexadecimal is a counting system that uses base 16, and it's		23	Q. Do both of these emails appear to be emails dated March 10,	
24	just like our counting system, it starts at zero and goes up to		24	2009?	
25	nine, but then for ten through 16, it uses letters. So to		25	A. Yes.	
HCKTTUZ3	DeCapua - Direct	Page 6566	HCKTTUZ3	DeCapua - Direct	Page 6568
1	count in hexadecimal you go start at zero and go to nine, and		1	Q. And are they the same subject line?	
2	the next would be A, B, C, D, E, and F and it stops at F.		2	A. So one of them is the reply.	
3	MS. GRISWOLD: I would like to pass up to witness what		3	Q. They both say audit of Enable Invest Ltd?	
4	is marked for identification as Government Exhibit 3550, 3551		4	A. Yes.	
5	and 3552, and the Court as well.		5	MR. JACKSON: Excuse me, your Honor, may I ask the	
6	Also passing up what is marked for identification as		6	Court to ask the government to briefly read the portion of our	
7	Government Exhibit 34, which is a stipulation between the		7	stipulation that relates to redactions?	
8	parties. With the Court's permission I would like to read		8	THE COURT: Yes, that might be appropriate,	
9	Government Exhibit 34.		9	Ms. Griswold.	
10	THE COURT: Are you offering it?		10	MS. GRISWOLD: Yes, your Honor. I believe the portion	
11	MS. GRISWOLD: Yes, your Honor.		11	of the stipulation that Mr. Jackson is referring to is in	
12	THE COURT: Is there any objection to Government		12	paragraph one.	
13	Exhibit 34?		13	THE COURT: Yes, is that what you wish read at this	
14	MR. JACKSON: No objection at all.		14	point, Mr. Jackson?	
15	THE COURT: Government Exhibit 34 is received.		15	MR. JACKSON: Yes, your Honor, thank you.	
16	(Government's Exhibit 34 received in evidence).		16	THE COURT: All right.	
17	THE COURT: And you may read it.		17	MS. GRISWOLD: On the morning of November 7, 2017,	
18	MS. GRISWOLD: Thank you.		18	Omar Amanat's attorneys first produced copies of emails that	
19	At this point I'm going to read paragraphs four and		19	were ultimately admitted into evidence at trial in redacted	
20	five of Government Exhibit 34.		20	form as Amanat Exhibits 908, 9002, 9010, and 9013. These	
21	THE COURT: Do you want them displayed to the jury?		21	documents were redacted before being offered at the request of	
22	MS. GRISWOLD: Yes, please, your Honor.		22	the government.	
23	Paragraph four. On November 30, 2017, at the request		23	MR. JACKSON: Thank you very much.	
24	of the government, Omar Amanat's attorneys logged onto a Yahoo		24	MS. GRISWOLD: If we could put back up Government	
25	web mail account belonging to Mr. Amanat and produced copies of		25	Exhibit 3550 next to Amanat Exhibit 908.	

UNITED STATES OF AMERICA, V  
KALEIL ISAZA TUZMAN, et al.,

December 20, 2017

HCKTTUZ3	DeCapua - Direct	Page 6569	HCKTTUZ3	DeCapua - Direct	Page 6571
<p>1 BY MS. GRISWOLD:</p> <p>2 Q. So the 3550, this has header information for this email?</p> <p>3 A. That's correct.</p> <p>4 Q. And it includes more email content than is reflected in</p> <p>5 Amanat Exhibit 908?</p> <p>6 A. Yes.</p> <p>7 Q. But it does include the email content in the redacted</p> <p>8 Amanat Exhibit 908, correct?</p> <p>9 A. Yes. Yeah, there's things missing from the content in 908.</p> <p>10 Q. So focusing on 3550, which is the email produced by the</p> <p>11 defendant with the header information, did you take a closer</p> <p>12 look at the header information for this March 10, 2009</p> <p>13 document?</p> <p>14 A. I did.</p> <p>15 Q. I want to direct you in particular to the message ID.</p> <p>16 MS. GRISWOLD: If we could highlight that at the top.</p> <p>17 Q. Did you take a closer look in particular at the message ID?</p> <p>18 A. I did.</p> <p>19 Q. What did you look at and what did you find?</p> <p>20 A. So I was asked to look at this email and try to determine</p> <p>21 whether or not it was authentic. And of course, as I said, an</p> <p>22 email header could have some very useful things that help make</p> <p>23 that determination. And looking at this header there wasn't a</p> <p>24 lot of information, so I zoomed in on the message ID, because I</p> <p>25 know that sometimes a message ID can have, for instance, a</p>	<p>1 MS. GRISWOLD: I would like to show the witness what</p> <p>2 is marked for identification as Government Exhibit 3579A, and</p> <p>3 the Court.</p> <p>4 Q. Do you recognize what is marked as Government</p> <p>5 Exhibit 3779A?</p> <p>6 A. I do.</p> <p>7 Q. How do you recognize it?</p> <p>8 A. This is something I created.</p> <p>9 Q. Is it a chart that you created based on your review of</p> <p>10 message IDs from Omar Amanat Blackberry from Maiden's computer?</p> <p>11 A. That's correct.</p> <p>12 Q. Is it accurate?</p> <p>13 A. Yes.</p> <p>14 MS. GRISWOLD: The government offers Government</p> <p>15 Exhibit 3579A.</p> <p>16 MR. JACKSON: No objection, Judge.</p> <p>17 THE COURT: 3579A is received.</p> <p>18 (Government's Exhibit 3579A received in evidence)</p> <p>19 MS. GRISWOLD: Permission to publish?</p> <p>20 THE COURT: Yes.</p> <p>21 Q. So this chart is entitled select emails present on Stephen</p> <p>22 Maiden's computer around March 10, 2009, sent from Omar Amanat</p> <p>23 with a Blackberry message ID. Is that an accurate title for</p> <p>24 the content?</p> <p>25 A. It is.</p>				
<p>HCKTTUZ3</p> <p>1 timestamp.</p> <p>2 Looking at the message ID, it looks just like a random</p> <p>3 number, but there's way to make sense of these numbers and try</p> <p>4 to figure out what they mean. And so what I did is first I</p> <p>5 looked, and this message ID is from a Blackberry, so when you</p> <p>6 send an email from a Blackberry, Blackberry tags this message</p> <p>7 ID on to the email. And I looked for more examples of</p> <p>8 Blackberry message IDs then and they looked just like this.</p> <p>9 Q. Are when you said you were looking for examples, were you</p> <p>10 provided access to a set of emails?</p> <p>11 A. I was. So first I looked online and I saw they were all</p> <p>12 consistent, and I wanted to make sure they were consistent</p> <p>13 around this exact time period, March 2009, because I know</p> <p>14 sometimes you can -- a company can change the format of its</p> <p>15 message ID. And I knew that the government had in its</p> <p>16 possession some emails that were recovered from a guy named</p> <p>17 Stephen Maiden's computer, and I knew that he was going to have</p> <p>18 emails from Omar Amanat.</p> <p>19 So I went to that computer and I sorted the messages</p> <p>20 by sender, and I exported every single message from Omar</p> <p>21 Amanat. And then when I got to my office I looked all the</p> <p>22 headers and carved out the ones sent from Omar Amanat with a</p> <p>23 Blackberry, and I just compared all the message IDs in a line,</p> <p>24 there were hundreds of them, and I noticed a pattern in those</p> <p>25 message IDs.</p>	<p>HCKTTUZ3</p> <p>1 Q. And this chart has less than several hundred emails. Does</p> <p>2 this include all of the emails that you reviewed from</p> <p>3 Mr. Maiden's computer?</p> <p>4 A. No, these are just the ones that were right around</p> <p>5 immediately around the timestamp.</p> <p>6 Q. Can you walk the jury through the columns in this chart and</p> <p>7 what it is that they indicate?</p> <p>8 A. So the first column is date and time sent. Now from the</p> <p>9 header I just plucked the date, it's very clear cut, I just</p> <p>10 copied and pasted it into this column for each email. The</p> <p>11 sender, same thing, I just took the sender field from the</p> <p>12 message header. In this case, every single one is Omar Amanat.</p> <p>13 Then I took the message ID, again, from the message</p> <p>14 header I just copied and pasted that field and populated this</p> <p>15 column. And then we're jumping a little bit ahead of ourselves</p> <p>16 here, but then there were two additional columns, one is for a</p> <p>17 hidden timestamp that I found within the message ID, and the</p> <p>18 next column is the conversion from epoch time, which is what</p> <p>19 the hidden timestamp is in, into something that is human</p> <p>20 readable.</p> <p>21 MS. GRISWOLD: Could we highlight the very first row.</p> <p>22 Q. And can you make sense of this row? This is an email that</p> <p>23 you found on Mr. Maiden's computer?</p> <p>24 A. Yes.</p> <p>25 Q. And that you understand to be authentic?</p>				

UNITED STATES OF AMERICA, V  
KALEIL ISAZA TUZMAN, et al.,

December 20, 2017

HCKTTUZ3	DeCapua - Direct	Page 6573	HCKTTUZ3	DeCapua - Direct	Page 6575
<p>1 A. Yes.</p> <p>2 Q. And can you walk through the comparison of the first</p> <p>3 column, date time sent, with the last column, timestamp</p> <p>4 conversion?</p> <p>5 A. Absolutely. So as I was -- as I mentioned before, when I'm</p> <p>6 looking at all the message IDs I noticed that pattern, and the</p> <p>7 pattern is the second number in the message ID after the first</p> <p>8 hyphen, it was incrementing as dates were going into the</p> <p>9 future. So a really old message would have -- this number</p> <p>10 would be lower and a newer message the message would be higher,</p> <p>11 and I saw it was just incrementing.</p> <p>12 And I immediately recognized it at this point, this a</p> <p>13 timestamp, an epoch hidden timestamp within the message ID.</p> <p>14 And because of that, I knew I could use that, it would have</p> <p>15 some value as helping me figure out if the email here is</p> <p>16 actually authentic. And so what I did is I started converting</p> <p>17 the message IDs from epoch time, which again is just a number</p> <p>18 which represents the number of seconds since January 1st, 1970,</p> <p>19 into something that I could read and make sense of. On the far</p> <p>20 right-hand side of the spreadsheet you could see the timestamp</p> <p>21 and timestamp conversion, which is just me making that</p> <p>22 conversion.</p> <p>23 Then I recognized that -- I knew it was a timestamp, I</p> <p>24 didn't know what it was a timestamp of. But once I made this</p> <p>25 conversion I started looking at the sent date, and I saw that</p>	<p>1 or not this email, the Tuesday, March 10, 2009 email, is</p> <p>2 authentic?</p> <p>3 A. Yeah, it's a fake email.</p> <p>4 Q. Are you confident in that opinion?</p> <p>5 A. I am.</p> <p>6 Q. Now besides this one example that's highlighted on the</p> <p>7 screen, were you able to find any other examples in the</p> <p>8 hundreds of Blackberry messages from Omar Amanat to Mr. Maiden</p> <p>9 on his computer where the timestamp conversion did not match up</p> <p>10 with the date and time sent?</p> <p>11 A. No.</p> <p>12 Q. Were you able to find any other examples besides this one?</p> <p>13 A. Not from the ones on Stephen Maiden's computer.</p> <p>14 MS. GRISWOLD: Let's turn to Government Exhibit 3552,</p> <p>15 please, and if we could put that up side by side with Amanat</p> <p>16 Exhibit 9002.</p> <p>17 Q. From the stipulation that I read, Government Exhibit 3552</p> <p>18 on the left is the December 2nd, 2008 email with the header</p> <p>19 information as provided by the defendant?</p> <p>20 A. That's correct.</p> <p>21 Q. And did you take a closer look at the message ID in this</p> <p>22 email?</p> <p>23 A. I did.</p> <p>24 Q. And what did you find?</p> <p>25 A. So again, now that I knew there was a hidden timestamp in</p>				
HCKTTUZ3	DeCapua - Direct	Page 6574	HCKTTUZ3	DeCapua - Direct	Page 6576
<p>1 the timestamp conversion for every single email was within</p> <p>2 seconds of the sent date. So therefore I concluded that this</p> <p>3 hidden timestamp that's in the message ID is a reflection of</p> <p>4 when the email was sent.</p> <p>5 Q. For the hundreds of emails that you reviewed, putting aside</p> <p>6 the exhibits that are in evidence in this case, did the date</p> <p>7 time stamp line up when you did the timestamp conversion, did</p> <p>8 they match?</p> <p>9 A. Yes.</p> <p>10 MS. GRISWOLD: If we could pull up the highlighted</p> <p>11 row, please.</p> <p>12 Q. Is this the message ID information that was pulled from</p> <p>13 Government Exhibit 3550 that was provided by the defendant?</p> <p>14 A. Yes.</p> <p>15 Q. Can you walk us through what you noticed when you analyzed</p> <p>16 this message ID?</p> <p>17 A. So now that after reviewing the emails I found on Stephen</p> <p>18 Maiden's computer, I knew what to expect, and so I compared it</p> <p>19 to the emails that I was provided to determine the authenticity</p> <p>20 of. And I saw that the message ID, the hidden timestamp within</p> <p>21 the message ID, when I made the conversion it came to</p> <p>22 July 23rd, 2009, which is not the date that the email was sent.</p> <p>23 Q. Based on your review of this header information and all of</p> <p>24 the other information on Mr. Maiden's computer that you've</p> <p>25 testified about, are you able to offer an opinion as to whether</p>	<p>1 the message ID, I immediately zoomed in on it. And the first</p> <p>2 thing I noticed is the message ID -- the hidden timestamp is</p> <p>3 absurd, it's actually a date in the future, and I knew it</p> <p>4 couldn't possibly be real.</p> <p>5 Q. If we could go to what is marked for identification as</p> <p>6 Government Exhibit 3579B.</p> <p>7 Do you recognize Government Exhibit 3579B as another</p> <p>8 chart you prepared for your testimony?</p> <p>9 A. Yes.</p> <p>10 Q. And is it accurate?</p> <p>11 A. It is accurate.</p> <p>12 Q. Does it relate to December 2nd, 2008 analysis?</p> <p>13 A. It does.</p> <p>14 MS. GRISWOLD: The government offers Government</p> <p>15 Exhibit 3579B.</p> <p>16 MR. JACKSON: No objection.</p> <p>17 THE COURT: Government Exhibit 3579B is received.</p> <p>18 (Government's Exhibit 3579B received in evidence)</p> <p>19 BY MS. GRISWOLD:</p> <p>20 Q. The title of this chart is select emails present on Stephen</p> <p>21 Maiden's computer around December 2nd, 2008, sent from Omar</p> <p>22 Amanat with a Blackberry message ID.</p> <p>23 What does this chart reflect?</p> <p>24 A. It reflects the same thing as -- the same information as</p> <p>25 the previous chart, it is just comparing the December 2nd, 2008</p>				

UNITED STATES OF AMERICA, V  
KALEIL ISAZA TUZMAN, et al.,

December 20, 2017

HCKTTUZ3	DeCapua - Direct	Page 6577	HCKTTUZ3	DeCapua - Direct	Page 6579
1	email provided by the defendant to all the other emails I found		1	that the message was not sent at the time and date indicated.	
2	on the Stephen Maiden computer.		2	Maybe that's a better way to -- maybe that's more precise.	
3	Q. Around that time period?		3	MR. NAFTALIS: Your Honor, one of the issues is there	
4	A. Around that time period.		4	is no evidence it was ever even sent, so I don't want to leave	
5	Q. Putting aside the highlighted ones, for all of the other		5	the misimpression. The point is it was fabricated, and the	
6	ones on the chart, did the date and time stamp time sent, the		6	point it is that it was never moved between computers.	
7	first column, match up when you did the timestamp conversion?		7	MR. JACKSON: But what the Court just said encompassed	
8	A. Yes, within an approximation.		8	what you said. The fact that it was not sent at the time and	
9	Q. What about the highlighted row, if we could blow that up,		9	date it purports to have been sent encompasses --	
10	what did you find when you looked at the hidden timestamp for		10	MR. NAFTALIS: That assumes it was ever sent though.	
11	the Tuesday, December 2nd, 2008, header information?		11	MR. JACKSON: It does not, it doesn't assume that, and	
12	A. As I said before, it indicates a date that's in the future.		12	that's really what his opinion goes to scientifically.	
13	Q. October 29, 2087?		13	THE COURT: I think it's implicit, because according	
14	A. Yes.		14	to agent's chart, it was sent in 2087.	
15	Q. Based on your review of this user ID -- sorry, message ID		15	MR. NAFTALIS: Maybe I'm being too sensitive to it,	
16	information from the December 2nd, 2008 email reflected in		16	but the whole point is that we're -- the jury doesn't know that	
17	Amanat Exhibit 9002, are you able to offer an opinion as to		17	you can upload -- we haven't completed the whole steps. We	
18	whether or not this email is authentic?		18	would contest that this email even moved between two computers,	
19	A. Yes.		19	so to limit his testimony to it was sent leaves the impression	
20	MR. JACKSON: Objection.		20	for Mr. Jackson to argue maybe there was computer error when it	
21	THE COURT: Grounds?		21	moving between the computers. And the point is it was	
22	MR. JACKSON: Goes beyond the scope of what he's		22	fabricated and never actually moved. It's an impossibility.	
23	testifying to.		23	MS. GRISWOLD: The jury heard the term "authenticity"	
24	THE COURT: I'll hear you at sidebar.		24	throughout the trial, and I think here, if you don't want me to	
25	Ladies and gentlemen, we'll take a brief recess.		25	say is it fake, I think it would be accurate to say based on	
HCKTTUZ3	DeCapua - Direct	Page 6578	HCKTTUZ3	DeCapua - Direct	Page 6580
1	Don't discuss the case, we'll get back to you shortly.		1	this message ID, can you offer an opinion to whether or not	
2	(At sidebar)		2	this email is authentic.	
3	THE COURT: So I didn't understand how this was		3	MR. JACKSON: Again, I think it's enormous --	
4	different than his previous question.		4	authentic does not actually answer the question, it goes	
5	MR. JACKSON: Your Honor, frankly, I anticipated the		5	beyond -- there's a whole bunch of things that are encompassed	
6	first question would come in slightly differently, and I should		6	in that that goes beyond the scope of what he can actually	
7	have objected at that time. But I do think that this -- I		7	testify to.	
8	understand that the question was posed at the hearing, and I		8	MS. GRISWOLD: It was fabricated. He would say that	
9	understand for the purposes of hearing that type of sort of		9	message ID was typed in and everything was changed because it's	
10	blunt questioning could be potentially useful to the Court. I		10	not possible.	
11	didn't think that the government would ask a question that went		11	MR. JACKSON: He could say -- I think he could offer	
12	that far in terms of the conclusion that Special Agent DeCapua		12	that testimony and say my opinion is that this message ID was	
13	is able to offer. And I think that the conclusion that he's		13	fabricated. I think that everything beyond that is beyond the	
14	able to offer really is that the message ID on here he does not		14	scope of his expertise.	
15	believe is authentic. He can't testify that the message in its		15	THE COURT: The other piece of it would be the email	
16	entirety is inauthentic. There's no basis for that.		16	was not sent at the time and date indicated. He could	
17	MS. GRISWOLD: I think he can, I think it can be two		17	certainly testify to that.	
18	questions if you want, but I think what he would say is this		18	MR. WILLIAMS: Can she clarify whether or not he could	
19	message ID is fake, and when you have a fake message ID, in his		19	conclude that the email was ever sent to clear up any potential	
20	opinion -- and he's set forth his qualifications, his opinion		20	implicit suggestion that the message ID was inaccurate but it	
21	is that that means that the email is fake.		21	may have been sent earlier in time?	
22	MR. JACKSON: But there's no scientific basis for		22	THE COURT: Can he testify that the message was never	
23	that, it's entirely possible --		23	sent?	
24	THE COURT: I guess it turns into the question of what		24	MS. GRISWOLD: That particular message -- I am happy	
25	do you mean by "fake." So what we mean by that, I think, is		25	to confer with him, but I believe, yes, he's saying that	

UNITED STATES OF AMERICA, V  
KALEIL ISAZA TUZMAN, et al.,

December 20, 2017

HCKTTUZ3	DeCapua - Direct	Page 6581	HCKTTUZ3	DeCapua - Direct	Page 6583
1	message ID is a message ID that doesn't make sense that tells		1	(Jury present)	
2	him that the email itself was a fabricated email. When you say		2	THE COURT: You may proceed.	
3	"that message," I think he could testify that that specific		3	MS. GRISWOLD: Thank you, your Honor.	
4	message was never sent.		4	If we could please put up Government Exhibit 3579B.	
5	THE COURT: I don't see how he could testify it was		5	BY MS. GRISWOLD:	
6	never sent, because theoretically it could have been sent,		6	Q. Before the break, Special Agent DeCapua, we were talking	
7	right?		7	about the message ID that you identified for the Tuesday,	
8	MS. GRISWOLD: It could have been sent.		8	December 2nd, 2008 email that is in evidence in redacted form	
9	THE COURT: This particular communication was not		9	as Amanat Exhibit 902. I want to go back to your testimony	
10	sent. He couldn't testify that the content of that email was		10	about what opinions you're able to offer concerning your	
11	not sent.		11	analysis.	
12	MS. GRISWOLD: Was never sent?		12	First, let me ask you, are you able to offer an	
13	THE COURT: Yeah, who knows? That's not a question		13	opinion as to whether or not this message ID for this email was	
14	that he sought to answer, let's put it that way.		14	fabricated?	
15	MR. WILLIAMS: which is why I suggested the question:		15	A. Yes.	
16	Can you conclude, based on this message ID, whether or not this		16	Q. And what is that opinion?	
17	email was ever sent? And presumably he would say no, I cannot		17	A. It's fake.	
18	make that conclusion.		18	MS. GRISWOLD: Let's put up Amanat Exhibit 9002. If	
19	MS. GRISWOLD: How about to offer an opinion that the		19	we could highlight the date, please.	
20	message ID was fabricated and that this particular email was		20	Q. Based on your testimony that the message ID is fake, are	
21	not sent on December 2nd, 2008?		21	you able to offer an opinion as to whether or not this email	
22	MR. JACKSON: I'm good with that. That's acceptable.		22	was sent on Tuesday, December 2nd, 2008?	
23	THE COURT: And I think that's clear.		23	A. Yes.	
24	MR. JACKSON: Your Honor, I want to -- related to		24	Q. What's that opinion?	
25	that, I would personally like to ask that -- can we clarify the		25	A. It wasn't sent.	
HCKTTUZ3	DeCapua - Direct	Page 6582	HCKTTUZ3	DeCapua - Direct	Page 6584
1	record on his prior answer with regard to saying that it's		1	Q. And I assume your opinion -- well, let me ask, what's your	
2	fake? I think that that exact same language is what really		2	opinion as to whether or not it was sent in 2087?	
3	should be limited in his opinion in regard to both		3	A. It definitely was not sent in 2087.	
4	communications.		4	Q. You testified earlier about your training and	
5	MS. GRISWOLD: I think you could elicit that on cross.		5	investigations analyzing email headers in the context of	
6	There was no objection and I think there was foundation for it.		6	determining if emails were spoofed. Do you recall that	
7	THE COURT: I don't think we can go back to that, but		7	testimony?	
8	you're welcome to cross-examine on that.		8	A. I do.	
9	MR. JACKSON: Thank you, Judge.		9	(Continued on next page)	
10	THE COURT: We'll take a brief recess.		10		
11	(Recess taken)		11		
12	THE COURT: Agent DeCapua can retake the stand.		12		
13			13		
14			14		
15			15		
16			16		
17			17		
18			18		
19			19		
20			20		
21			21		
22			22		
23			23		
24			24		
25			25		

UNITED STATES OF AMERICA, V  
KALEIL ISAZA TUZMAN, et al.,

December 20, 2017

HckWtuz4	DeCapua - Direct	Page 6585	HckWtuz4	DeCapua - Direct	Page 6587
<p>1 BY MS. GRISWOLD:</p> <p>2 Q. In that analysis, is the Message-ID a focus of your</p> <p>3 analysis?</p> <p>4 A. It is.</p> <p>5 Q. Why?</p> <p>6 A. So when you're trying to determine whether an email is</p> <p>7 faked or spoofed or fraudulent, as I mentioned before, you look</p> <p>8 to the header, and there's certain things in the header that</p> <p>9 you focus in on. And as I mentioned before, you focus in on</p> <p>10 the Message-ID, and one of the gold standards for determining,</p> <p>11 determining that an email is fake is you find two emails in an</p> <p>12 account with the same Message-ID. Message-IDs are always</p> <p>13 unique. They're always unique. If you find two with the same</p> <p>14 Message-ID, you know one of them is fake.</p> <p>15 When you're spoofing an email or when you're trying to</p> <p>16 create a fake email, you go into the header and you change</p> <p>17 things in the header, and people know that a Message-ID can't</p> <p>18 be the same.</p> <p>19 MR. JACKSON: Objection.</p> <p>20 THE COURT: Sustained.</p> <p>21 BY MR. JACKSON:</p> <p>22 Q. So a Message-ID is important to your analysis whether or</p> <p>23 not an email has been fabricated?</p> <p>24 A. Yes, it's common for a Message-ID to be changed by someone</p> <p>25 fabricating an email because they don't want it to match the --</p>	<p>1 Q. Did you investigate this Message-ID?</p> <p>2 A. I did.</p> <p>3 Q. What, if anything, struck you about it?</p> <p>4 A. No. 1, it was created most likely with an Apple Mail</p> <p>5 client, which is on an iPhone; it's on Apple computers. And I</p> <p>6 just identified the Message-ID as being the format that Apple</p> <p>7 Mail uses.</p> <p>8 The other thing that struck me is you can break this</p> <p>9 Message-ID into two parts and you can break it up using the</p> <p>10 "at" symbol that's right before Amanat Capital. So what's</p> <p>11 interesting is everything before the "at" symbol. It looks</p> <p>12 like a random jumble of numbers and letters, but that format is</p> <p>13 something very significant in computer science. This is a</p> <p>14 UUID, which I defined earlier. It stands for a universal</p> <p>15 unique identifier, and they all have the same format. There's</p> <p>16 going to be eight characters, a hyphen, four characters, a</p> <p>17 hyphen, four more characters, a hyphen, four more characters, a</p> <p>18 hyphen, and then 12 characters. And this is something found</p> <p>19 throughout computer science on all different platforms. It's</p> <p>20 also known as a GUID, which stands for globally unique</p> <p>21 identifier, and I know that a GUID or a UUID is in something</p> <p>22 called hexadecimal, which I defined earlier.</p> <p>23 Q. Can you just remind the jury what hexadecimal is?</p> <p>24 A. Hexadecimal is the way that computers count, and it allows</p> <p>25 for the digits zero through 9 and the letters A through F.</p>				
HckWtuz4	DeCapua - Direct	Page 6586	HckWtuz4	DeCapua - Direct	Page 6588
<p>1 MR. JACKSON: Objection.</p> <p>2 THE COURT: Sustained.</p> <p>3 You can't testify as to what goes on in someone else's</p> <p>4 mind, so whenever you lapse into topics of what someone else is</p> <p>5 thinking, there's going to be an objection and it's going to be</p> <p>6 sustained.</p> <p>7 THE WITNESS: I apologize.</p> <p>8 BY MR. JACKSON:</p> <p>9 Q. In the course of your analysis of Message-IDs to determine</p> <p>10 whether or not emails have been fabricated, have you identified</p> <p>11 situations where the Message-ID has been changed?</p> <p>12 A. Yes.</p> <p>13 Q. Let's go to Government Exhibit 3551, the third email that</p> <p>14 you were asked to analyze.</p> <p>15 MS. GRISWOLD: Put it up on the screen, please, and</p> <p>16 put it side by side with Amanat Exhibit 9013.</p> <p>17 Q. On the left-hand side, Government Exhibit 3551, is this the</p> <p>18 header information that you were provided for this March 26,</p> <p>19 2012, exhibit?</p> <p>20 A. Yes, it is.</p> <p>21 Q. And based on the stipulation that we read, this is the</p> <p>22 header information provided by the defendant for this email?</p> <p>23 A. That's correct.</p> <p>24 Q. I want to direct your attention to the Message-ID.</p> <p>25 MS. GRISWOLD: Could I ask Ms. Pyun to highlight it.</p>	<p>1 Nothing else.</p> <p>2 THE COURT: Could you go back and explain how it is</p> <p>3 that you were able to determine that this was created on an</p> <p>4 Apple Mail client?</p> <p>5 THE WITNESS: Sure. So, there's resources that I</p> <p>6 looked at where it will say this is a pattern of the Message-ID</p> <p>7 for this specific client or this is a pattern for Message-ID</p> <p>8 for this specific client, and this specific pattern for a</p> <p>9 Message-ID is associated with Apple Mail clients. And also, I</p> <p>10 tested that, and I've looked at emails that I know have been</p> <p>11 sent from Apple Mail, including ones I've sent myself, ones</p> <p>12 that have been sent from other people's pages in the regular</p> <p>13 course of business, and they fit this pattern, every single one</p> <p>14 of them.</p> <p>15 THE COURT: When you say this pattern, could you</p> <p>16 identify what you see on this exhibit, Government Exhibit 3551,</p> <p>17 where on it is the pattern that you're talking about that</p> <p>18 indicates it's Apple?</p> <p>19 THE WITNESS: The pattern is the UUID, which is</p> <p>20 everything before the "at" symbol and then the "at" symbol and</p> <p>21 then everything after the "at" symbol, which is a domain name.</p> <p>22 THE COURT: All right. Go ahead, Ms. Griswold.</p> <p>23 BY MR. JACKSON:</p> <p>24 Q. And you testified that you looked at some other emails to</p> <p>25 make sure that you were correct that this was an Apple Mail, is</p>				

UNITED STATES OF AMERICA, V  
KALEIL ISAZA TUZMAN, et al.,

December 20, 2017

HckWtuz4	DeCapua - Direct	Page 6589	HckWtuz4	DeCapua - Direct	Page 6591
1	that correct?		1	Q. Starting with 908, what is your opinion as to whether or	
2	A. I did.		2	not this email was sent on Tuesday, March 10, 2009?	
3	Q. Was that limited to messages from this case, or did you		3	A. No.	
4	take a broader universe?		4	MR. JACKSON: Objection, your Honor. Asked and	
5	A. I took a very broad universe to include emails from -- sent		5	answered.	
6	to me in the regular course of business, to emails that I		6	THE COURT: Overruled.	
7	created myself using one of the accounts that I set up and		7	This is a wrap-up, I take it.	
8	other emails in my possession where I would just quickly run		8	MS. GRISWOLD: It is, your Honor.	
9	through and confirm that an Apple Mail client always has this		9	THE COURT: Yes. It's overruled.	
10	type of UUID.		10	BY MR. JACKSON:	
11	Q. So you testified that the hexadecimal can only have zero		11	Q. What was your answer?	
12	through 9 or A through F. Do I have that right?		12	A. It's a fake email.	
13	A. That's correct.		13	MR. JACKSON: Objection.	
14	Q. And in this case, what did you notice about this Message-ID		14	THE COURT: The question was, Agent, whether Amanat	
15	that struck you, based on those parameters?		15	Exhibit 908, you could offer an opinion as to whether or not	
16	A. I noticed that in the, in the fifth set of numbers after		16	that email was sent on Tuesday, March 10, 2009. That was the	
17	the fourth hyphen, it does not conform to a standard for UUID,		17	question.	
18	which I would expect it all to be hexadecimal. There's two		18	THE WITNESS: It was not sent.	
19	characters, they're V's, which there's no reason a V should be		19	MS. GRISWOLD: If we could zoom up on 9013.	
20	there, in a hexadecimal number.		20	Q. Are you able to offer an opinion as to whether that was	
21	Q. Based on your review of this Message-ID and your		21	sent on Monday, March 26, 2012.	
22	familiarity with hexadecimal characters, are you able to offer		22	A. It was not sent.	
23	an opinion as to whether or not this Message-ID was fabricated?		23	Q. And finally, Amanat Exhibit 9002, are you able to offer an	
24	A. Yes. It's fake.		24	opinion as to whether this email was sent on Tuesday, December	
25	MS. GRISWOLD: If we could zoom out and show the		25	2, 2008, at 11:07 p.m.?	
HckWtuz4	DeCapua - Direct	Page 6590	HckWtuz4	DeCapua - Cross	Page 6592
1	entire exhibit, Amanat Exhibit 9013.		1	A. It was not sent.	
2	Q. Based on your testimony that the user ID is fake, are you		2	MS. GRISWOLD: No further questions, your Honor.	
3	able to offer an opinion whether or not --		3	THE COURT: All right. Cross-examination.	
4	THE COURT: It's the Message-ID that's fake, right?		4	CROSS-EXAMINATION	
5	MS. GRISWOLD: Yes, your Honor. If I said something		5	BY MR. JACKSON:	
6	else, I misspoke.		6	Q. Good afternoon, Special Agent DeCapua.	
7	THE COURT: I heard you to say user ID.		7	A. Good afternoon.	
8	MS. GRISWOLD: Oh, I misspoke.		8	Q. Special Agent DeCapua, I know you're a very accomplished	
9	THE COURT: Yes. Could you reask the question,		9	federal agent. I want to ask you a few questions about your	
10	please.		10	training specifically related to the issues you've testified	
11	MS. GRISWOLD: Certainly.		11	about.	
12	Q. Based on your testimony that the Message-ID for this email		12	I'd also like to ask, I'd like to respectfully ask, I'm	
13	was fake, are you able to offer an opinion as to whether or not		13	going to try to phrase all my questions, unless it's necessary	
14	this email was sent on Monday, March 26, 2012?		14	otherwise, in the format of yes or no. So I would ask if you	
15	A. It was not.		15	can answer it yes or no, please do so. If you can't, please	
16	MS. GRISWOLD: If we could put up on the screen Amanat		16	let me know if you can't answer yes or no.	
17	Exhibit 910 -- 9010. Thank you, Mr. Urbanczyk.		17	A. OK.	
18	Q. Special Agent DeCapua, were you provided with any header		18	Q. Thank you, Agent.	
19	information for this email?		19	Now, I want to just start off by asking you, you	
20	A. No.		20	attended Indiana University, correct?	
21	Q. So you were unable to do the analysis you did on the other		21	A. For my graduate degree, that's correct.	
22	emails?		22	Q. Where did you get your bachelor's degree?	
23	A. That's right.		23	A. It was DePaul University.	
24	MR. JACKSON: And if we could bring up on one screen		24	Q. OK, so you went to DePaul for undergrad and then you went	
25	Amanat Exhibits 908, 9002 and 9013.		25	to Indiana University for graduate school, correct?	

UNITED STATES OF AMERICA, V  
KALEIL ISAZA TUZMAN, et al.,

December 20, 2017

HckWtuz4	DeCapua - Cross	Page 6593	HckWtuz4	DeCapua - Cross	Page 6595
<p>1 A. That's correct.</p> <p>2 Q. In neither of those did you get a degree in computer science, right?</p> <p>4 A. I did not get a degree in computer science.</p> <p>5 Q. In neither of those did you have a minor in computer science?</p> <p>7 A. I did not minor in computer science.</p> <p>8 Q. In either your graduate or your undergraduate education, did you take any classes on network engineering?</p> <p>10 A. Not on network engineering.</p> <p>11 Q. You've never taken classes that qualified you to be a network engineer, correct?</p> <p>13 A. Not in college or graduate studies.</p> <p>14 Q. OK, well, you're not a network engineer, right?</p> <p>15 A. Correct.</p> <p>16 Q. And network engineer is a type of technology professional who has a specific technological understanding necessary to construct and analyze the networks that are utilized for email systems, correct?</p> <p>20 A. Yes.</p> <p>21 Q. Now, just to be clear, have you taken any formal classes on engineering?</p> <p>23 A. Yes.</p> <p>24 Q. Now, one of the things that you talked about earlier was some of your professional experience, right?</p>		<p>1 THE COURT: Sustained.</p> <p>2 Q. 2014?</p> <p>3 A. That's correct.</p> <p>4 Q. And so in 2014, you began to focus with particularity on some of the types of cyber issues that have been your recent focus, right?</p> <p>7 A. So, I can't answer that in yes or no.</p> <p>8 Q. That's fine. That's fine. I'll come back to that. Let me get more information. The point being 2014 is when you joined the cyber squad?</p> <p>11 A. That's right.</p> <p>12 Q. You've been doing that work for the past three years?</p> <p>13 A. Yes.</p> <p>14 Q. And I'm correct that that's when you started taking the classes that we saw on your résumé from GIAC, right?</p> <p>16 A. That's correct.</p> <p>17 Q. Now, GIAC is not a governmental agency, correct?</p> <p>18 A. Correct.</p> <p>19 Q. GIAC is a, it's a nonprofit organization, right?</p> <p>20 A. I believe so, yes.</p> <p>21 Q. And just to be clear, and I have a couple of questions about GIAC, but you've never held an appointment as professor in network engineering or any other type of computer science at any university, have you?</p> <p>25 A. No.</p>			
HckWtuz4	DeCapua - Cross	Page 6594	HckWtuz4	DeCapua - Cross	Page 6596
<p>1 A. Yes.</p> <p>2 Q. You've never worked at Blackberry, correct?</p> <p>3 A. Correct.</p> <p>4 Q. You've never worked at Apple, correct?</p> <p>5 A. That's correct.</p> <p>6 Q. You've never worked at Microsoft?</p> <p>7 A. Correct.</p> <p>8 Q. You've never worked at any of the companies that actually build the computer infrastructure that you've been testifying about today, right?</p> <p>11 A. That's correct.</p> <p>12 Q. What did you do before you were a federal agent?</p> <p>13 A. I was an investigator for the state of Indiana.</p> <p>14 Q. Doing what type of investigations?</p> <p>15 A. It was primarily securities fraud, financial fraud, money laundering.</p> <p>17 Q. OK. And so after that, you came to the FBI, in 2009, right?</p> <p>19 A. That's correct.</p> <p>20 Q. And for the first several years that you were at the FBI, you weren't focused on the cyber squad that you're a part of now, right?</p> <p>23 A. That's right.</p> <p>24 Q. You didn't transfer to that until 2015, right?</p> <p>25 MS. GRISWOLD: Objection.</p>		<p>1 Q. And you've never been published in any journal related to computer sciences, right?</p> <p>3 A. No.</p> <p>4 Q. You've never been published in any journal related to network engineering, correct?</p> <p>6 A. No.</p> <p>7 Q. You've never been published in any journal that relates to the architecture of email systems, right?</p> <p>9 A. No.</p> <p>10 Q. And just going back to GIAC, GIAC has been the heart of your formal training on these issues, right?</p> <p>12 A. That's correct.</p> <p>13 Q. The total amount of time that you have spent in formal training in GIAC is about two weeks, am I correct?</p> <p>15 A. You are incorrect.</p> <p>16 Q. I'm incorrect?</p> <p>17 A. That's right.</p> <p>18 Q. OK. What is the total amount of time that you've spent in formal training in GIAC?</p> <p>20 THE COURT: Could we find out what you mean by formal training?</p> <p>22 MR. JACKSON: Yes, your Honor.</p> <p>23 THE COURT: Do you mean training at GIAC, or do you mean something else?</p> <p>25 MR. JACKSON: I mean training at GIAC.</p>			

UNITED STATES OF AMERICA, V  
KALEIL ISAZA TUZMAN, et al.,

December 20, 2017

HckWtuz4	DeCapua - Cross	Page 6597	HckWtuz4	DeCapua - Cross	Page 6599
1 Q. Let me ask you. What is the total amount of time that 2 you've spent in courses at GIAC? 3 A. So, just -- quickly, just to differentiate for the record, 4 GIAC is the certifying body. They don't put on courses. The 5 body that puts on courses is something called SANS, and the 6 total amount of time that I sat in a class, probably six weeks. 7 Q. OK. So you've sat in classes for SANS for about six weeks 8 for your GIAC certifications? 9 A. Thereabout. 10 Q. And you have several different GIAC certifications that we 11 went through? 12 A. That's correct. 13 Q. Now, to pass a GIAC course, you only have to take one 14 class, right, one test? 15 A. Yes. 16 Q. And you have to get 69 percent or better on that test, 17 right? 18 A. So, each exam has a different threshold. I believe the 69 19 percent is for the really difficult -- it's a networking exam, 20 which I passed. Most of them are closer to like the 70 to 80 21 percent threshold. 22 Q. OK. You don't know specifically what the threshold was for 23 each one of the GIAC certifications in your résumé, right? 24 A. Not right now, no. 25 Q. OK, but it's your testimony that generally it hovers	1 level, right? 2 A. Yes. It's just a test. It's actually not a class. 3 Q. Right. And the certification is called GIAC security 4 expert, right? 5 A. That's correct. 6 Q. That's a certification that you don't have? 7 A. It's a certification I don't have currently. 8 Q. OK. Now, the fact of the matter is you were describing in 9 your direct examination some of your work with email headers, 10 correct? 11 A. That's correct. 12 Q. And am I correct that, just going back earlier to one of 13 the things that you talked about with the judge -- 14 MR. JACKSON: Can we focus on 3579-B. 15 Q. And this is one of the documents that you created for this, 16 right? 17 A. Correct. 18 Q. For your testimony? 19 A. Correct. 20 Q. And there is a time stamp here. There's a column for the 21 time stamp, correct? 22 A. That's right. 23 Q. With the exception of December 2, 2008, email that's 24 highlighted, all of the other emails you got off Mr. Maiden's 25 computer, right?				
HckWtuz4	DeCapua - Cross	Page 6598	HckWtuz4	DeCapua - Cross	Page 6600
1 somewhere between 69 percent and about 80 percent, is that 2 right? 3 A. Yes. 4 Q. And to be clear, there are different levels of GIAC 5 certifications, right? 6 A. Correct. 7 Q. There's a beginner level? 8 A. Yes. 9 Q. And then there are two intermediate levels. One is called 10 intermediate and one is called advanced, right? 11 A. So -- I don't know. I don't know what you're talking 12 about. 13 Q. OK. There's an intermediate level, right, in GIAC? 14 A. There are intermediate-level courses. There's one course 15 that is definitely the beginner level, which I actually did not 16 take, and then there are the intermediate level and then the 17 advanced courses. 18 Q. And then there's a level above the advanced that's called 19 expert courses, right? 20 A. So, there's not an expert course. There's an expert 21 certification. The GFE is what I believe you're referring to. 22 Q. Have you seen the GIAC road map for certification that is 23 listed on the GIAC website? 24 A. I have. 25 Q. And you're aware that it identifies that there's an expert	1 A. Yes. 2 Q. And when you took a look at those, you said you took a look 3 at hundreds of them, right? 4 A. That's correct. 5 Q. How many exactly did you take a look at? 6 A. So, I don't know the exact number. I had them all in a 7 gigantic test file, and then I automated the process of looking 8 through them all, and I didn't count the exact number. 9 Q. OK. Did you take notes as you were doing this process? 10 A. No. 11 Q. OK. 12 A. Other than populating this. 13 Q. But you put all of those in a gigantic text file, the 14 hundreds you were looking at? 15 A. Correct. 16 THE COURT: And these were all BlackBerry messages, 17 right? 18 THE WITNESS: Yes. 19 Q. What did you do with that text file? 20 A. So, I ran some scripts on it just to quickly parse out the 21 information I'm interested in, particularly the part that is 22 the hidden time stamp, so then I put that all in another column 23 without having to type them in all by hand. 24 Q. I guess my question specifically was, did you save that 25 text file?				

UNITED STATES OF AMERICA, V  
KALEIL ISAZA TUZMAN, et al.,

December 20, 2017

HckWtuz4	DeCapua - Cross	Page 6601	HckWtuz4	DeCapua - Cross	Page 6603
1 A.	I would assume so, but I'm not 100 percent sure if I did.		1	MS. GRISWOLD: Objection to form. Test out.	
2 Q.	Did you save the scripts that you ran in connection		2	THE COURT: Sustained.	
3 with the text file?			3	Q. You didn't actually make a determination for each one of	
4 A. No.			4	the specific emails that you looked at whether the time stamp	
5 Q. OK. So you ran the scripts; did you write down what you			5	matched up with the sent time?	
6 saw when you ran the scripts?			6	THE COURT: That's confusing. You mean the ones on	
7 THE COURT: Could you explain what you mean by			7	the chart or all the ones he looked at?	
8 scripts?			8	MR. JACKSON: I'm talking about all of the emails that	
9 THE WITNESS: So, there's some built-in scripting			9	he looked at, your Honor.	
10 programs in Linux, which is the computer I was -- it's a type			10	A. All the emails I looked at, I -- to my satisfaction, I was	
11 of operating system that I was using to do this analysis			11	happy that the time stamp reflected the date the email was	
12 because you can quickly parse through large text files, and by			12	sent.	
13 large I mean humongous. These were, just to open the text			13	Q. OK. Let's put aside satisfaction. My question is, did you	
14 file, it would crash the computer, so I needed a way to			14	actually run the number that you found, what you believe is the	
15 systematically quickly parse through it, and Linux has some			15	hidden time stamp in order to convert it into a time that is	
16 built-in tools that you can use to script. And by script, I			16	human readable for all of these hundreds of messages?	
17 just mean it's an automated process that takes the manual work			17	A. Yes.	
18 out of things, and so I can write a script that says, Using the			18	Q. So you actually ran the conversion?	
19 tool built into Linux to ingest every single one of these			19	A. Yes.	
20 Message-IDs and throw out everything other than the hidden time			20	Q. Did you preserve that anywhere?	
21 stamp number that I'm interested in, and then that script will			21	A. I don't think so. I don't know.	
22 say take that hidden time stamp number and create a new text			22	Q. You're not sure?	
23 file where all these hidden time stamps are just there, and			23	A. I'm not sure.	
24 then I can take them and copy and paste them into a column.			24	Q. OK. You knew that you were doing this in anticipation of	
25 THE COURT: I see.			25	testifying in court, right?	
HckWtuz4	DeCapua - Cross	Page 6602	HckWtuz4	DeCapua - Cross	Page 6604
1 BY MR. JACKSON:			1 A.	Well, that's why I built this spreadsheet.	
2 Q. Now, one of the things you said is that when you ran these			2 Q.	I see, but I'm talking about what's not on the spreadsheet.	
3 scripts, I think your direct testimony was they all came close			3	You knew that that was all in anticipation of your testifying	
4 to the sent time, and I think your words were "within an			4	in court, correct?	
5 approximation"?			5	A. Correct.	
6 A. That's correct.			6	Q. And so you ran hundreds of bits of analysis, and you're	
7 Q. When you say within an approximation, how big was the gap			7	telling me that you didn't take any notes?	
8 that you saw in the messages that are not on your sheet from			8	THE COURT: Sustained.	
9 the sent time that was listed in the email?			9	Q. OK. You didn't preserve what you ran in any way?	
10 A. So, after -- I didn't look through every single one, but			10	MS. GRISWOLD: Objection. May we have a sidebar?	
11 after taking a sampling, I saw that it was consistently a few			11	MR. JACKSON: Your Honor, I'm going to move on to	
12 seconds to maybe like a minute or two, at most, different from			12	another topic. We can talk about it on a break.	
13 the actual sent time of the email.			13	THE COURT: All right.	
14 Q. I'm confused, because you said, I thought, in your direct			14	BY MR. JACKSON:	
15 testimony, that you went through hundreds of these and saw that			15	Q. Now, one of the things you also have said --	
16 the sent time consistently matched up with what you described			16	MR. JACKSON: Can you get, I don't know the exhibit	
17 as the time stamp. Right?			17	number, the third --	
18 A. Right. So I would eyeball it. I would scroll through and			18	Q. By the way, you first came up with this two nights ago,	
19 say, all right, these all say March 3, and these are March 3,			19	right?	
20 I'm going through, and I'm not looking at each second, you			20	A. That's correct.	
21 know, time stamp for every single one.			21	Q. So before two nights ago, you had never come up with this	
22 Q. So you didn't actually test out for all these hundreds that			22	theory before?	
23 you went through, you didn't actually test out whether or not			23	MS. GRISWOLD: Objection. Form. This theory.	
24 the time in the time stamp that you found matched up with the			24	THE COURT: Sustained.	
25 sent time?			25	Q. All of the analysis we're talking about, right, you came up	

UNITED STATES OF AMERICA, V  
KALEIL ISAZA TUZMAN, et al.,

December 20, 2017

HckWtuz4	DeCapua - Cross	Page 6605	HckWtuz4	DeCapua - Cross	Page 6607
1	with two nights ago?		1	Q. From a computer standpoint, from a coding standpoint?	
2	MS. GRISWOLD: Objection.		2	Well, just to be clear, you don't actually -- you're not a	
3	THE COURT: Grounds.		3	person who has ever actually done the coding for the creation	
4	MS. GRISWOLD: Form and as to what he means by this		4	of Message-IDs, right?	
5	analysis. It's too vague.		5	A. I have not.	
6	THE COURT: Can you rephrase your question?		6	Q. But you are aware that the coding connected to Message-IDs	
7	MR. JACKSON: Yes, Judge.		7	can be utilized to create a unique Message-ID in a number of	
8	Q. During your direct testimony, Special Agent DeCapua, you		8	different ways, right?	
9	described your realization that there was a hidden time stamp		9	MS. GRISWOLD: Objection. Foundation.	
10	within certain Blackberry messages, correct?		10	THE COURT: Sustained.	
11	A. That's correct.		11	Q. Now, the fact of the matter is one of the things that you	
12	Q. You came to that conclusion two nights ago, right?		12	testified about on your direct examination was this concept of	
13	A. That's correct.		13	a UUID?	
14	Q. And before that, you had never done any analysis where you		14	A. That's correct.	
15	determined that there was a purported hidden time stamp in the		15	Q. And I think your testimony -- first of all, your testimony	
16	Blackberry system, right?		16	has been that a Message-ID has to be unique, right?	
17	A. That's right.		17	A. That's correct.	
18	Q. And to be clear, you've never conferred with anyone at		18	Q. That's not precisely correct, right?	
19	Blackberry to verify your theory, right?		19	A. I believe, according to the authoritative RFC that	
20	A. That's correct.		20	addresses Message-IDs, the one thing it says a Message-ID must	
21	Q. And so no one on your cyber squad had ever heard of this		21	be is unique.	
22	theory before, correct?		22	Q. Right.	
23	THE COURT: What theory?		23	THE COURT: And when you say authoritative RFC, what	
24	MR. JACKSON: Withdrawn, your Honor.		24	is it you're talking about? What's the RFC?	
25	Q. You're not aware of any literature anywhere that describes		25	THE WITNESS: So when the Internet was developed,	
HckWtuz4	DeCapua - Cross	Page 6606	HckWtuz4	DeCapua - Cross	Page 6608
1	the hidden time stamp that you're talking about that you see in		1	the -- it was a bunch of universities that were just exchanging	
2	these messages, correct?		2	information, saying how should we make our computers talk to	
3	A. So, there is literature that describes that time stamps are		3	each other, and the convention for sharing information and for	
4	sometimes embedded in Message-IDs.		4	publishing it was something called an RFC, which stands for	
5	Q. But you're not aware of any literature that describes the		5	request for comment.	
6	specific hidden time stamp that you've been talking about,		6	Now, over time, the request-for-comments that have	
7	right?		7	been published by -- there's a nonprofit agency, I don't know	
8	THE COURT: I don't understand the question.		8	what the name of it, they have become the authoritative	
9	Q. Well, you've been talking about a hidden time stamp that		9	guidebook for what specific protocols must have and what they	
10	you've been using in these Blackberry messages, right?		10	should have and generally how computers are supposed to talk	
11	A. Correct.		11	over a network. And so when developers are trying to figure	
12	Q. You're not aware of anywhere that it's documented that that		12	out how they should code their software, the most authoritative	
13	hidden time stamp appears in Blackberry messages?		13	place where they get the answers as what they must and should	
14	A. Correct. I found it.		14	have, they go to the RFC where things are published.	
15	Q. You found it on your own?		15	BY MR. JACKSON:	
16	A. Yes.		16	Q. Thank you. I'm glad we got to the creation of the	
17	Q. Now, one of the things that you know, and I think you		17	Internet, because you're aware of how UUIDs were developed,	
18	testified on direct, is that companies can alter the way that		18	right?	
19	Message-IDs are created within their computer systems, right?		19	MS. GRISWOLD: Objection. Foundation.	
20	A. That's correct.		20	MR. JACKSON: I'm asking a question. He's been	
21	Q. That comes down to a coding decision, correct?		21	talking about his understanding of the history of the Internet.	
22	A. Yes.		22	THE COURT: The objection is overruled.	
23	Q. And there are numerous ways of creating a Message-ID,		23	Are you aware how UUIDs were developed?	
24	right?		24	THE WITNESS: No.	
25	A. Correct.		25	BY MR. JACKSON:	

UNITED STATES OF AMERICA, V  
KALEIL ISAZA TUZMAN, et al.,

December 20, 2017

HckWtuz4	DeCapua - Cross	Page 6609	HckWtuz4	DeCapua - Cross	Page 6611
1	Q. Have you heard of the Apollo company?		1	it came from an Apple Mail client, right?	
2	A. No.		2	A. Correct.	
3	Q. You're not familiar with that at all?		3	Q. And in fact, you can't look at a UUID and determine	
4	A. No.		4	definitively that it came from an Apple Mail computer, can you?	
5	Q. Have you heard of Hewlett-Packard?		5	A. You can't.	
6	A. Yes.		6	Q. Right. It's impossible because there are many different	
7	Q. You know that Hewlett-Packard is one of the companies that		7	ways a UUID can be created, right?	
8	was involved in the early creation of UUIDs?		8	A. Yes.	
9	A. I have no idea.		9	Q. A software engineer can create, can design programming that	
10	Q. You're not familiar with that. OK.		10	creates a UUID that has the same format as the one you looked	
11	Are you familiar with what is known as the Open Software		11	at that's not an Apple Mail UUID, right?	
12	Foundation?		12	MS. GRISWOLD: Objection. Foundation.	
13	A. I've heard of it, yes.		13	THE COURT: Sustained.	
14	Q. You've heard of it, right? That's the organization that		14	Q. Now, your testimony was that all UUIDs are in hexadecimal,	
15	deals with standards for UUIDs, correct?		15	correct?	
16	A. I don't know.		16	A. Correct.	
17	Q. You're not familiar with that?		17	Q. And what is the source of your belief? Can you point us to	
18	A. No.		18	any authority that says that all UUIDs are hexadecimal?	
19	Q. OK. Have you ever looked into any of the standards		19	MS. GRISWOLD: Objection to form.	
20	associated with UUIDs?		20	THE COURT: Overruled.	
21	MS. GRISWOLD: Objection. Form.		21	A. Yes, there's lots --	
22	THE COURT: Sustained.		22	THE COURT: I guess there are two questions there.	
23	Q. What is the source of your training on UUIDs?		23	MR. JACKSON: Let me break it up, your Honor.	
24	A. Mostly it's in Windows Registry Forensics. A UUID is used		24	Q. What is the source of your understanding that all UUIDs are	
25	very frequently, and I don't -- I never got into the history of		25	in hexadecimal?	
HckWtuz4	DeCapua - Cross	Page 6610	HckWtuz4	DeCapua - Cross	Page 6612
1	them or why they look the way they are, but they're one of		1	A. So, first, it's just been through observation, and second,	
2	those things that when you see them you know them.		2	it's been through research. I believe the Wikipedia posts for	
3	Q. Let's back up from that. What I'm trying to understand is		3	hexadecimal says or the Wikipedia post for UUID says "is in	
4	how is it that when you see a UUID, you know it? Where did you		4	hexadecimal."	
5	learn that?		5	Q. You're relying on Wikipedia? That's your testimony?	
6	THE COURT: Let's start with, what do you mean by		6	MS. GRISWOLD: Objection.	
7	Windows Registry Forensics? What is that, and what is the		7	THE COURT: His testimony was that he was relying on	
8	relationship between that and your ability to identify UUIDs?		8	his own observation and Wikipedia.	
9	THE WITNESS: So, Windows keeps a database inside		9	Q. OK, so your observations plus Wikipedia, right?	
10	their operating system that's called a registry, and inside the		10	A. Plus other sources that don't come to mind right now, but	
11	registry has different things related to the operating system.		11	it's an established standard.	
12	For instance, system mate is in the registry. And as a		12	Q. What other sources? Can you give us any of them?	
13	database it has something called a key, which is a number that		13	A. You could probably open up an introductory computer science	
14	represents each field in the database, and something that's		14	textbook, and it will describe what a UUID and have	
15	commonly used in the Windows registry to act as a key is a		15	information.	
16	UUID.		16	Q. Sir, your theory --	
17	BY MR. JACKSON:		17	MS. GRISWOLD: Objection.	
18	Q. OK. So I want to know, where did you learn about the		18	THE COURT: Sustained.	
19	UUIDs?		19	Q. Your testimony that all UUIDs are in hexadecimal is based	
20	A. From studying digital forensics.		20	on the idea -- first of all, you understand, right, that a UUID	
21	Q. Is it something that you learned in your GIAC classes?		21	doesn't have to be in base 16? Right?	
22	A. Yes, it was something that was discussed in GIAC classes,		22	MS. GRISWOLD: Objection. Foundation.	
23	not the history or formation, but the fact that this is a UUID.		23	MR. JACKSON: He's testified about it. I'm asking the	
24	Q. Right. To be clear, no one ever taught you in GIAC classes		24	question.	
25	that you could look at a UUID and determine definitively that		25	THE COURT: Overruled.	

HckWtuz4	DeCapua - Cross	Page 6613	HckWtuz4	DeCapua - Cross	Page 6615
1	You can answer that question.		1	Q. OK. Is this something that you've ever come across in your	
2	A. They do have to be in base 16.		2	Google searching?	
3	Q. Sir, isn't it a fact that UUIDs can be created in base 32?		3	THE COURT: In his Google searching? Is that what you	
4	A. UUIDs?		4	said?	
5	Q. Yes, UUIDs.		5	MR. JACKSON: Yes, your Honor.	
6	A. No.		6	MS. GRISWOLD: Objection to form. When he says this,	
7	Q. OK. Sir, isn't it a fact that UUIDs can also be created in		7	does he mean this particular article?	
8	base 64?		8	THE COURT: That's what you mean, right?	
9	A. My understanding is all UUIDs are in hexadecimal.		9	MR. JACKSON: Yes, Judge.	
10	Q. Do you know what base 32 is?		10	A. This particular blog post, no.	
11	A. I know it as a concept but not in practice.		11	Q. OK. Have you come across blog posts where people are	
12	Q. Educate us on what you know about it as a concept, please.		12	discussing programming that they've done to create UUIDs in	
13	A. So, as a concept, like I said, we count in base 10. It's		13	base 64?	
14	an counting system that goes up to 10. Computers count in base		14	A. No.	
15	16, which is a counting system that that goes up to the number		15	MS. GRISWOLD: Objection. Foundation.	
16	16 and incorporates letters up to F in order to represent		16	MR. JACKSON: It's a question.	
17	numbers higher than 10. Base 32 would be a counting system		17	THE COURT: He's answered it. He said no.	
18	that counts up to 32. Base 64 would be a counting system that		18	Next question.	
19	counts up to 64.		19	BY MR. JACKSON:	
20	THE COURT: But have you ever seen or do you have		20	Q. The fact of the matter is you understand that if a UUID was	
21	experience with either base 32 or base 64?		21	created in base 64, it would include all the letters in the	
22	THE WITNESS: No, and I don't see them in practice in		22	alphabet?	
23	digital forensics.		23	MS. GRISWOLD: Objection.	
24	BY MR. JACKSON:		24	THE COURT: Sustained.	
25	Q. Well, you've done some Google searches in connection with		25	MR. JACKSON: Your Honor, he's testified.	
HckWtuz4	DeCapua - Cross	Page 6614	HckWtuz4	DeCapua - Cross	Page 6616
1	your testimony today, right?		1	THE COURT: Sustained.	
2	A. Yes.		2	BY MR. JACKSON:	
3	Q. Didn't you come across numerous articles online that		3	Q. Putting aside the creation of a UUID, do you know what base	
4	indicate UUIDs can be created in base 32 and base 64?		4	64 is?	
5	A. No.		5	A. So, yes.	
6	Q. You've never seen that?		6	Q. OK. In base 64, all of the letters of the alphabet are	
7	A. I've never seen that.		7	used, correct?	
8	Q. OK. I want to show you something that's marked as Amanat		8	A. Yes, and a couple symbols also.	
9	Exhibit 97.		9	Q. OK. And the difference between base 32 and base 64 is that	
10	MR. JACKSON: Let me show this just to the witness.		10	in base 32, you use all capital letters, right?	
11	Your Honor, I'm going to pass a copy to the Court.		11	MS. GRISWOLD: Objection. Foundation.	
12	Q. Please take a look at that, sir, and then I have some		12	MR. JACKSON: He said he knows what it is.	
13	questions.		13	MS. GRISWOLD: 32.	
14	A. OK.		14	THE COURT: Actually, he hasn't testified that he	
15	Q. Is this an article that you've reviewed before?		15	knows what base 32 is, so the objection's sustained.	
16	A. No.		16	MR. JACKSON: Thank you, Judge.	
17	Q. OK, but having looked at this, does this alter your opinion		17	Q. Agent DeCapua, do you know what base 32 is?	
18	at all about whether or not a UUID can be created in base 32 or		18	A. So, it's not something that's used. Base 64 --	
19	base 64?		19	Q. I'm just asking whether or not you know what it is? Do you	
20	MS. GRISWOLD: Objection. Foundation.		20	know what it is?	
21	THE COURT: Sustained.		21	A. As a concept, yes.	
22	Q. Let me show you a different document that I'm going to mark		22	Q. As a concept. OK. Let's just talk conceptually. In base	
23	as Amanat Exhibit 98.		23	32, you use the digits zero through 9 as well as all the	
24	Do you see this, sir?		24	letters of the alphabet in capitals?	
25	A. I do.		25	A. I have no idea.	

HckWtuz4	DeCapua - Cross	Page 6617	HckWtuz4	DeCapua - Cross	Page 6619
1	MS. GRISWOLD: Objection. Foundation.		1	THE COURT: Sustained.	
2	MR. JACKSON: He said he had no idea.		2	Q. Now, one of the things that programming believes	
3	THE COURT: OK. The transcript's garbled. I'm		3	Message-IDs can do is adapt the format related to the	
4	sustaining the objection.		4	Message-ID when network conditions change, right?	
5	BY MR. JACKSON:		5	MS. GRISWOLD: Objection to form.	
6	Q. Sir, can you -- the Wikipedia page --		6	THE COURT: Sustained. You can ask the question, but	
7	THE COURT: I'm sorry?		7	I don't understand its present format.	
8	MR. JACKSON: The Wikipedia page.		8	MR. JACKSON: OK, Judge.	
9	Q. It's a fact that nowhere on the Wikipedia page for UUIDs		9	Q. Sir, you understand network conditions in terms of the	
10	does it say that a UUID has to be in base 16, correct?		10	amount of traffic are something that can impact the transfer of	
11	A. I don't know for sure, but UUIDs are in base 16.		11	an email message, right?	
12	Q. Sir, if you don't know for sure, that's fine. That's my		12	THE COURT: That's just too vague. Do you mean	
13	question. Do you know?		13	traffic, or do you mean something else?	
14	A. If it's in the Wikipedia article?		14	MR. JACKSON: I mean traffic, your Honor.	
15	Q. Yes.		15	THE COURT: OK. Reask the question and focus on	
16	A. I don't know.		16	traffic.	
17	Q. The fact of the matter also, sir, is that --		17	MR. JACKSON: OK.	
18	MR. JACKSON: If we could take a quick look at		18	Q. You're familiar --	
19	Government Exhibit 3551.		19	THE COURT: Actually, it's volume of traffic, right?	
20	THE COURT: Government Exhibit 3951?		20	MR. JACKSON: Yes, your Honor.	
21	MR. JACKSON: 3551, your Honor.		21	Q. You're familiar with the concept of network traffic, right?	
22	THE COURT: 3551.		22	A. Yes.	
23	MR. JACKSON: Yes, and if we could zoom in on the top		23	Q. Network traffic, when it increases, impacts the movement of	
24	half of that.		24	emails from one server to another, right?	
25	Q. To be very clear, you eyeballed this and thought it looked		25	A. It could slow down.	
HckWtuz4	DeCapua - Cross	Page 6618	HckWtuz4	DeCapua - Cross	Page 6620
1	like a UUID, right?		1	Q. Right, and one of the things that a programmer can do is	
2	MS. GRISWOLD: Objection.		2	alter the information that would appear in Message-ID,	
3	THE COURT: Are we putting 3551 up on the screen,		3	depending on network traffic, correct?	
4	because I don't have anything?		4	MS. GRISWOLD: Objection. Foundation and form.	
5	MR. JACKSON: It's on the screen, your Honor. It may		5	THE COURT: Sustained.	
6	be a glitch.		6	MR. JACKSON: Your Honor, could we have a sidebar?	
7	THE COURT: It wasn't on my screen.		7	THE COURT: Yes.	
8	MR. JACKSON: Sorry.		8	(Continued on next page)	
9	THE COURT: Can you ask the question again.		9		
10	MR. JACKSON: Yes.		10		
11	Q. You testified that you eyeballed this, right?		11		
12	MS. GRISWOLD: Objection. Mischaracterizes the		12		
13	testimony about this Message-ID.		13		
14	THE COURT: Sustained.		14		
15	BY MR. JACKSON:		15		
16	Q. The fact of the matter is you can't state definitively that		16		
17	this is a unique UUID, can you?		17		
18	A. When looking at it --		18		
19	Q. I'm sorry. I'm just asking, yes or no, you can't state		19		
20	definitively that this is a UUID?		20		
21	A. Well, it's not a UUID because it has a V in it.		21		
22	Q. Right. And the fact of the matter is it is possible to		22		
23	create a Message-ID that has this format that is not a UUID,		23		
24	right?		24		
25	MS. GRISWOLD: Objection. Foundation.		25		

HckWtuz4	DeCapua - Cross	Page 6621	HckWtuz4	DeCapua - Cross	Page 6623
1	(At sidebar)		1	to make foundational questions every time I ask a question, I	
2	THE COURT: Now, you have established that he's not a		2	have no way of knowing what he does and does not know, and I	
3	coder, he's never studied coding, he's never done any coding,		3	have to be allowed to explore that.	
4	and now you're asking him what programmers can do. Not only is		4	THE COURT: You did have the opportunity to question	
5	there no foundation, but the limited foundation that is in the		5	him on two separate occasions, so it's not entirely accurate to	
6	record suggests that he doesn't know anything about this. If		6	say you don't know anything about this witness. You've heard	
7	you want to get into, and this has been a recurring problem.		7	him testify twice about the subject matter that we're talking	
8	If you want to get into these area, you've got to lay a		8	about now, and I say that not to minimize the situation.	
9	foundation that he has an understanding, and then we can get to		9	MR. JACKSON: No, I understand, Judge.	
10	the specific question, but you're starting with a question		10	THE COURT: What we're doing here is quite unusual	
11	without any background as to what he knows and what he doesn't		11	given that the problem came up in the middle of trial, but I	
12	know.		12	did want to say for the record it's not entirely accurate to	
13	MR. JACKSON: Judge, here's my problem. I definitely		13	say that you haven't had prior exposure to the witness, because	
14	tended to undermine his credentials, because I don't think this		14	he's testified at length twice before.	
15	witness knows what he's talking about, but he testified on		15	MR. JACKSON: I agree, Judge.	
16	direct extensively about some very problematic conclusions, and		16	THE COURT: But I'm sensitive to what you've said.	
17	I don't feel like a foundational objection on cross-examination		17	I am going to give him some latitude. If I think that	
18	of an expert witness who has testified as to these subjects is		18	the background is so lacking in foundation that it will be hard	
19	appropriate. If he doesn't know the answer, he should just say		19	to interpret what his answer is, I'll sustain the objection,	
20	"I don't know the answer." I mean, the whole point of my		20	and if I don't, I will allow it. I am going to allow him some	
21	question is to determine whether he knows the answer. To say		21	latitude, though.	
22	lack of foundation, that's more appropriate for direct		22	MS. GRISWOLD: I understand, your Honor. I just would	
23	examination or cross-examination of someone who is a fact		23	note for the record these appear to be network engineering and	
24	witness.		24	coding questions. I don't think the witness has this	
25	THE COURT: Let me make a couple of points. First of		25	background. I can't follow the questions. I don't think he	
HckWtuz4	DeCapua - Cross	Page 6622	HckWtuz4	DeCapua - Cross	Page 6624
1	all, the witness has been completely cooperative with you.		1	has the foundation for them.	
2	MR. JACKSON: Agreed.		2	THE COURT: That's another point. On a number of the	
3	THE COURT: He has not been hostile.		3	questions I've sustained objections to I didn't understand the	
4	MR. JACKSON: Agreed.		4	question, and you've gone out of your way to bring out that he	
5	THE COURT: He's not been obstructive. He's been		5	doesn't have credentials in these areas, and now you're asking	
6	completely cooperative.		6	him very technical questions. In demonstrating that he's not a	
7	MR. JACKSON: Agreed.		7	network engineer and he doesn't know anything about coding,	
8	THE COURT: So I have no reason to believe that if you		8	etc., etc., you've undermined your own ability to ask him these	
9	tried on lay a foundation with him that he would try to		9	very technical questions, because he's agreed with you. He's	
10	obstruct your examination in any way. All the evidence		10	not a network engineer, he hasn't studied computer science, he	
11	suggests so far is that he relied on observation and answered		11	hasn't done coding. And so when we get into these kinds of	
12	quite candidly whether he knows, for example, about programming		12	areas, it doesn't give me comfort that he has an adequate	
13	or whether he doesn't.		13	background to understand and to answer your questions.	
14	MR. JACKSON: I agree, Judge.		14	MR. JACKSON: Your Honor, I definitely appreciate	
15	THE COURT: The problem with just sort of dropping		15	that. I think the Court's ruling is very fair. I appreciate	
16	these questions in is it's hard to evaluate what his answer is		16	it. I just want to point out for an expert witness as opposed	
17	without knowing whether he's got any background in what it is		17	to a fact witness, even him saying that he does not know about	
18	we're talking about, and this particularly concerned me because		18	a particular subject is highly, highly relevant.	
19	you brought out coding, he doesn't do coding, and now you're		19	THE COURT: I don't disagree.	
20	asking him what programmers do. I just don't know that he has		20	MR. JACKSON: If he can say "I don't know," if he can	
21	that background.		21	say "I'm not familiar with that," it informs the jury's	
22	MR. JACKSON: I agree, Judge, but it's fundamentally		22	understanding of what the scope of his knowledge is.	
23	unfair for them to make foundation objections. I have no		23	THE COURT: I don't disagree.	
24	problem with Special Agent DeCapua's testimony. In my cross of		24	MS. GRISWOLD: I don't disagree either. And I think	
25	an expert, for whom I have no discovery, who I never met before		25	he's said that, he doesn't have knowledge in these areas.	

HckWtuz4	DeCapua - Cross	Page 6625	HckWtuz4	DeCapua - Cross	Page 6627
1	MR. JACKSON: That's fine, I just don't think a		1	(In open court)	
2	foundational objection is appropriate. I think it's perfectly		2	THE COURT: Please proceed, Mr. Jackson.	
3	appropriate for an expert witness to say "I don't know that,"		3	MR. JACKSON: Thank you very much, Judge.	
4	"that's beyond the area of my expertise," "I haven't looked		4	Q. Now, to be clear, Special Agent DeCapua, in the total	
5	into that," "I'm not familiar with that," and I'll accept his		5	amount of time that you've spent training on, in training on	
6	answers.		6	relevant, that is relevant to electronic evidence and	
7	THE COURT: But you're not asking whether he's		7	specifically email headers adds up to about two weeks, right?	
8	familiar with that or not. That's kind of the problem. Your		8	MS. GRISWOLD: Objection to form.	
9	refusal to ask foundation questions doesn't allow him, and		9	THE COURT: Sustained.	
10	you've made it very clear you want yes-or-no answers to your		10	Q. The total amount of time you've spent in formal classes	
11	questions and so it doesn't give him an opening to say "I'm		11	related to email headers adds up to about two weeks, correct?	
12	sorry, I don't know about that field." Your questioning and		12	A. That's correct.	
13	your style don't permit him to say that. If it did, we		13	(Continued on next page)	
14	wouldn't be up here.		14		
15	MR. JACKSON: OK. Judge, I'll just note, last, we		15		
16	have a bigger problem, but we'll address that at the break.		16		
17	THE COURT: While we're up here, can you give us a		17		
18	preview?		18		
19	MR. JACKSON: Yes, I can.		19		
20	THE COURT: OK.		20		
21	MR. JACKSON: There's an enormous 3500 problem in that		21		
22	I've got nothing --		22		
23	MS. GRISWOLD: I handed you the two pieces -- Special		23		
24	Agent DeCapua sent me an email with essentially the data from		24		
25	the charts that we created at, like, two in the morning, before		25		
HckWtuz4	DeCapua - Cross	Page 6626	HCKTTUZ5	DeCapua - Cross	Page 6628
1	we created them, and I handed those to you at the hearing.		1	BY MR. JACKSON:	
2	MR. JACKSON: I think we should talk about it at the		2	Q. Now just going back to 3511 --	
3	break.		3	THE COURT: 3511?	
4	(Continued on next page)		4	MR. JACKSON: Sorry, 3551, your Honor.	
5			5	If we could have 3551 again.	
6			6	Q. Can you point us to any authority that says that a message	
7			7	ID in this format has to come from Apple mail?	
8			8	A. There are articles online that -- forensic articles	
9			9	published by forensic groups that describe that Apple mail --	
10			10	MR. JACKSON: Sorry, I'm going to object.	
11			11	Q. I'm just asking: Can you identify an authority?	
12			12	THE COURT: You mean -- what do you mean by identify,	
13			13	the author of the article?	
14			14	MR. JACKSON: Sure, the author of the article, the	
15			15	name of the website, the name of the article.	
16			16	Q. Can you identify any article that says this?	
17			17	THE COURT: Do you want him to talk about websites or	
18			18	talk about authors or what?	
19			19	MR. JACKSON: Let's take it one by one, Judge.	
20			20	Q. Can you identify any published book that says that a	
21			21	message ID in this format has to come from Apple mail?	
22			22	A. Sitting here today, I can't think of any published book.	
23			23	Q. Okay. Can you identify a specific article anywhere that	
24			24	says a message ID in the format on Government Exhibit 3551 has	
25			25	to come from Apple mail?	

UNITED STATES OF AMERICA, V  
KALEIL ISAZA TUZMAN, et al.,

December 20, 2017

HCKTTUZ5	DeCapua - Cross	Page 6629	HCKTTUZ5	DeCapua - Cross	Page 6631
1 A.	I said there are articles, I cannot identify a specific one		1 Q.	It's not hexadecimal, right?	
2 sitting here today.			2 MS. GRISWOLD: Objection.		
3 Q.	Now you knew you were going to be testifying about this		3 THE COURT: I don't understand the question.		
4 particular subject, right?			4 Q.	This is not a hexadecimal format for this message ID,	
5 A.	That's correct.		5 right?		
6 Q.	And you were asked some questions about this at a separate		6 MS. GRISWOLD: Objection, asked and answered.		
7 proceeding, correct?			7 THE COURT: No, I will allow him to and answer.		
8 A.	That's correct.		8 Is this a hexadecimal format?		
9 Q.	Did you endeavor to try to find any specific articles that		9 THE WITNESS: No, because it has a V, but it's		
10 suggest that this message ID format necessarily indicates Apple			10 supposed to be.		
11 mail?			11 MR. JACKSON: So that gets to my question. That's		
12 A.	So now that you bring up the earlier hearing, I think we		12 where I was headed, Judge.		
13 did give you a copy of an article I found that identifies a			13 BY MR. JACKSON:		
14 GUID an at sign then domain name as belonging to Apple mail.			14 Q.	You can't say definitively that this is supposed to be	
15 Q.	I don't think that's accurate, but my question is not		15 hexadecimal, can you?		
16 whether or not Apple mail can create a GUID like this, but			16 A.	So I'm bound by common sense here, and when I see this	
17 whether or not the creation of a GUID with this format			17 format, 8-4-4-4-12, and everything conforms and looks like hex,		
18 necessarily indicates Apple mail?			18 and I read articles that say that it's supposed to be hex for		
19 THE COURT:	Could we refer to it as G-U-I-D? Because		19 Apple mail, and I do experiments myself and every single time I		
20 I'm not sure how the court reporter is supposed deal with			20 sent something from Apple mail it's in hex, it's UUID and has		
21 "GUID."			21 the domain name.		
22 MR. JACKSON:	Yes, your Honor, just using the		22 Q.	Do you understand there's a difference between all Apple	
23 witness's language.			23 mail emails being in hex and all hex emails necessarily		
24 Q.	It's probably better to refer to it as a UUID. Same thing,		24 indicate Apple mail, right? Those two things are not the same.		
25 right?			25 MS. GRISWOLD: Objection, form, foundation.		
HCKTTUZ5	DeCapua - Cross	Page 6630	HCKTTUZ5	DeCapua - Cross	Page 6632
1 A.	I agree, yes.		1 THE COURT: Do you understand the question?		
2 Q.	GUID and UUID are the same thing, correct?		2 THE WITNESS: I don't.		
3 A.	Same thing.		3 Q.	Let me rephrase that then. Your testimony is that all	
4 Q.	Just to confirm, Special Agent DeCapua, I want to confirm,		4 Apple mail message IDs are in hex, right?		
5 as you sit here now, you're not aware of any specific authority			5 A.	Just for clarification, this entire thing is the message	
6 that you can identify that says that a UUID in this format must			6 ID, so the beginning -- everything before the at sign is in		
7 come from Apple mail, right?			7 hex, everything after is just plain letters.		
8 A.	Sitting here today, no.		8 Q.	My only question is your testimony is that all Apple mail	
9 Q.	And you do concede that a message ID can contain these if		9 IDs are supposed to be in hex, right?		
10 it's not a base 16 message ID?			10 A.	Correct.	
11 MS. GRISWOLD:	Objection.		11 Q.	You can't say definitively that this is a Apple mail	
12 THE COURT:	Sustained.		12 message ID, right?		
13 Q.	You understand that not all messages IDs are in base 16,		13 MS. GRISWOLD: Objection, form.		
14 right?			14 THE COURT: Overruled.		
15 A.	Yes.		15 A.	There could be another service that uses the exact similar,	
16 Q.	Not all message IDs are hexadecimal, right?		16 and I wouldn't --		
17 A.	Correct.		17 Q.	So the answer is yes, right? You can't say definitively.	
18 Q.	And if a message ID is not hexadecimal, it could contain a		18 You agree with that?		
19 V, right?			19 A.	Correct.	
20 A.	Yes.		20 Q.	And the fact of the matter is there are numerous different	
21 Q.	And you can't say that the message ID in 3551 is		21 email services, right?		
22 necessarily supposed to be hexadecimal?			22 A.	Correct.	
23 THE COURT:	Supposed to be? Sustained.		23 Q.	There are lists of email clients available online that run	
24 Q.	Well, you can't say --		24 into the hundreds, right?		
25 MR. JACKSON:	Your Honor, it's a little bit --		25 A.	Yes.	

UNITED STATES OF AMERICA, V  
KALEIL ISAZA TUZMAN, et al.,

December 20, 2017

HCKTTUZ5	DeCapua - Cross	Page 6633	HCKTTUZ5	DeCapua - Cross	Page 6635
1 Q. There are numerous versions even of the specific email 2 clients that are associated with a particular company, right? 3 A. Could you repeat that question? 4 Q. For example, Blackberry has had various versions of its 5 email client that it used on the Blackberry, right? 6 A. So I don't know that for a fact. 7 Q. Well, you don't believe that they're still using the exact 8 same email operating system today as they were ten years ago, 9 do you? 10 A. I have no idea. 11 MS. GRISWOLD: Objection, foundation. 12 Q. You have no idea. But the point being you haven't gone out 13 and examined what the message ID format is for every email 14 client out there, have you? 15 A. No. 16 Q. So you don't know whether or not there's an email client 17 that creates a message ID that looks like this with a V, 18 correct? 19 A. So a message ID that looks like it's going to be a UUID but 20 then it changes something -- 21 Q. I'm not asking you whether it looks like a UUID, what I'm 22 saying is you don't know whether there are other email clients 23 that have a message ID that takes this approximate format but 24 contains Vs, correct? 25 A. I would be shocked to find that out.	1 MS. GRISWOLD: Objection. 2 THE COURT: Sustained. 3 Q. Can we go to 3579, please, 3579B. 4 So you see there's a hidden timestamp here, right? 5 A. That's correct. 6 Q. In your prior testimony you said that one of the things 7 that you looked at was you said that this looked like it could 8 potentially correspond with hexadecimal, right? 9 A. I don't think I said that -- or no, so you're referring to 10 a prior hearing. 11 Q. Yes, in a prior hearing. 12 A. Yes, I tried everything. 13 Q. One of the things that you did is explore whether or not 14 this could be a potentially hexadecimal timestamp, right? 15 A. Yes. 16 Q. Because you're aware that there is such a thing as a 17 hexadecimal timestamp that could potentially look like this on 18 the surface, right? 19 A. Yes. 20 Q. And your conclusion was if you converted it from the 21 hexadecimal timestamp via the methods that you're aware of, it 22 didn't come out to a time that you thought made sense, right? 23 A. So the methods that I'm aware of and the methods that I 24 tested are the most commonly used once. 25 Q. But there are a number of other different types -- there				
HCKTTUZ5	DeCapua - Cross	Page 6634	HCKTTUZ5	DeCapua - Cross	Page 6636
1 Q. You don't know, correct? 2 A. Correct. 3 Q. Now the fact of the matter is even with regard to your 4 testimony about the epoch timestamp, epoch timestamps can come 5 in many different formats, right? 6 A. That's correct. 7 Q. It's not just the format that you pointed out on your 8 chart, right? 9 A. The format I pointed out on the chart is overwhelmingly 10 used. It's the most common one. 11 Q. But there are other forms of epoch timestamps, right? 12 A. Yes. 13 Q. And there are other forms of timestamps in general that are 14 not epoch, right? 15 A. Yes. 16 Q. There are timestamps coded to the year 1900, correct? 17 A. January 1st, 1900. 18 Q. Bingo. There are timestamps coded to that, correct? 19 A. Correct. 20 Q. There are also message IDs that create randomization by 21 combining a timestamp in one of the formats available with some 22 other information, correct? 23 A. That's correct. 24 Q. You haven't -- for the message ID that you looked at for 25 the Blackberry message that you claim was irregular --	1 are a number of different methods for converting a hexadecimal 2 timestamp that you didn't explore, right? 3 A. All the methods of converting a hexadecimal timestamp I 4 tried. I'm not aware of any other methods. 5 Q. You can't say definitively, right, that isn't just a 6 randomly generated number on this, right? 7 MS. GRISWOLD: Objection to form. Which number are we 8 talking about? 9 MR. JACKSON: Withdrawn. 10 Q. On 3579B, with the December 2nd 2008 email, you can't say 11 definitively that the message ID software on Blackberry didn't 12 just generate a random number here, right? 13 A. So when every other instance -- 14 Q. I'm asking yes or no. 15 THE COURT: Can you answer it yes or no? 16 THE WITNESS: Could you repeat the question? 17 Q. You cannot say definitively that the message ID associated 18 with this message on December 2nd, 2008 was not just a randomly 19 generated number by this software. You agree with that, right? 20 A. Could it be? Sure. 21 Q. Okay. And the fact of the matter is you haven't gone back 22 to ask anyone at Blackberry -- 23 THE COURT: You've already asked him about Blackberry 24 over and over and over again. 25 MR. JACKSON: Judge, I'm very close to my end.				

UNITED STATES OF AMERICA, V  
KALEIL ISAZA TUZMAN, et al.,

December 20, 2017

HCKTTUZ5	DeCapua - Cross	Page 6637	HCKTTUZ5	DeCapua - Cross	Page 6639
<p>1 We could take that down.</p> <p>2 Q. Sir, you're also aware that there have been some very well</p> <p>3 publicized glitches associated with Blackberries and their</p> <p>4 timestamps, right?</p> <p>5 A. No.</p> <p>6 Q. You're aware of well-published glitches associated with</p> <p>7 epoch timestamps, correct?</p> <p>8 A. No.</p> <p>9 Q. You never heard of a glitch associated -- that creates a</p> <p>10 date of 2045 in computers?</p> <p>11 THE COURT: I thought we were talking about</p> <p>12 Blackberries.</p> <p>13 MR. JACKSON: I'm talking about epoch timestamps in</p> <p>14 general.</p> <p>15 Q. You heard of an epoch timestamp glitch that accidentally</p> <p>16 creates a date of 2045, right?</p> <p>17 MS. GRISWOLD: Objection to form, to "in computers."</p> <p>18 Q. Sir, epoch timestamps are used more broadly than just</p> <p>19 Blackberries, right?</p> <p>20 A. That's correct, but could I reanswer the question that you</p> <p>21 just asked me?</p> <p>22 Q. I don't even know what question we would be talking about.</p> <p>23 A. You asked me --</p> <p>24 Q. Let me just focus this on this question really quickly then</p> <p>25 we can address anything.</p>	<p>1 computers and Blackberries in 2009?</p> <p>2 THE COURT: Could you spell that for the court</p> <p>3 reporter, please?</p> <p>4 MR. JACKSON: E-T-I-S-A-L-A-T?</p> <p>5 A. I never heard of it.</p> <p>6 MR. JACKSON: May I have one moment, your Honor?</p> <p>7 THE COURT: Yes.</p> <p>8 (Pause)</p> <p>9 Q. Are you familiar with any viruses that infected</p> <p>10 Blackberries in 2009 for travelers in Dubai?</p> <p>11 A. No.</p> <p>12 Q. Now just going towards the end, your analysis on the</p> <p>13 document that is 3579A starts on March 10, 2009, right?</p> <p>14 A. What is --</p> <p>15 Q. 3579A.</p> <p>16 Before we get there, just one other question, did you</p> <p>17 look at the server traffic associated with the messages that</p> <p>18 you analyzed?</p> <p>19 MS. GRISWOLD: Objection, foundation.</p> <p>20 THE COURT: Overruled.</p> <p>21 A. If I understand you correctly, you mean the server traffic</p> <p>22 on January 27, 2009, for instance, for this email?</p> <p>23 Q. No, I guess what I'm asking is: Did you look at whether</p> <p>24 the server routes that were taken by the messages associated</p> <p>25 here, the messages that are marked as government exhibits, the</p>				
HCKTTUZ5	DeCapua - Cross	Page 6638	HCKTTUZ5	DeCapua - Cross	Page 6640
<p>1 You are aware epoch time is used in many different</p> <p>2 types of computers, right?</p> <p>3 A. That's correct.</p> <p>4 Q. And there have been well-publicized glitches associated</p> <p>5 epoch time, right?</p> <p>6 A. I'm familiar with just one.</p> <p>7 Q. What's the one you're familiar with?</p> <p>8 A. The one I'm familiar with is it's like a Y2K glitch, and</p> <p>9 it's basically when -- an epoch timestamp is just a big number,</p> <p>10 and eventually it will get to be such a big number that it will</p> <p>11 overflow the bounds of the specific piece of memory where the</p> <p>12 information is stored. And I think it's going to happen in</p> <p>13 like 2030 something, I'm not 100 percent sure about that, but</p> <p>14 there's discussions on what to do before then and whether it's</p> <p>15 going to cause the end of the world or kind of like Y2K.</p> <p>16 That's the one about publicized glitch I'm aware of.</p> <p>17 Q. 2030 something, right?</p> <p>18 A. That's what I think.</p> <p>19 Q. And you have seen publications online that talk about</p> <p>20 people -- their epoch timestamps glitching to create an</p> <p>21 incorrect date on their device of 2030-something, right?</p> <p>22 A. No, I have never seen that.</p> <p>23 Q. Have you researched that at all?</p> <p>24 A. No.</p> <p>25 Q. Okay. Have you heard of the Etisalat virus that infected</p>	<p>1 emails you were focused on, did you look at whether the server</p> <p>2 routes approximated the server routes that you saw in the other</p> <p>3 messages?</p> <p>4 THE COURT: Do you understand the question?</p> <p>5 A. I think you're asking: Did I look at the headers?</p> <p>6 Q. Yes.</p> <p>7 A. And look at the IP addresses contained in the headers?</p> <p>8 Q. Yes.</p> <p>9 A. So I could answer it in two parts. The first part is for</p> <p>10 the emails in question there were no server routing information</p> <p>11 because they were sent emails. So it's just what was on the</p> <p>12 defendant's computer that he gave to us.</p> <p>13 Q. So you weren't able to analyze that?</p> <p>14 A. I wasn't able to analyze it.</p> <p>15 Q. Let me ask you this, you're looking here at March 10, 2009,</p> <p>16 right?</p> <p>17 A. That's correct.</p> <p>18 Q. Now your comparator messages end January 30, 2009 and pick</p> <p>19 up again on March 11, 2009, right?</p> <p>20 A. That's correct.</p> <p>21 Q. So the email that you were focused in on is March 10, 2009</p> <p>22 from Omar Amanat to Steve Maiden, right?</p> <p>23 A. Yes.</p> <p>24 Q. Are you aware that there is a gap in Mr. Maiden's emails on</p> <p>25 his computer that goes exactly to March 10, 2009?</p>				

HCKTTUZ5	DeCapua - Cross	Page 6641	HCKTTUZ5	Page 6643
1 A. No.			1 (Jury not present)	
2 Q. You are not aware of that?			2 THE COURT: I received another note from the jury,	
3 A. No.			3 Court Exhibit 18, reads as follows: I have to take an online	
4 Q. That's something you never discussed with other FBI agents?			4 class for a job performance for Verizon on December 21st, 2017	
5 A. I think you asked me that question at a prior hearing and I			5 at 1:30 p.m. in my Bronx office. It's the last one. I thought	
6 said no.			6 we would be done. So I put off. It's a must. Signed Eric	
7 Q. After I asked you that, did you explore at all whether			7 Eleam.	
8 there was anything to be gleaned about that?			8 Second communication was just orally through	
9 A. No.			9 Mr. Ruocco, juror number four, Tara Charlton, asked me if it	
10 Q. Okay. When you were looking at the fact that the			10 becomes apparent that she will have to be excused that she ask	
11 message -- the comparator message is cut off at the end of			11 that she be excused today, given that she's got to try to get	
12 January and don't pick up again until the day after March 10,			12 to JFK Airport tomorrow. And so --	
13 2009, did you attempt to discover whether there was any missing			13 MS. GRISWOLD: Your Honor, may I speak to Mr. Maiden	
14 data that would be relevant to your investigation on			14 about the issue that we discussed this morning?	
15 Mr. Maiden's emails or computer?			15 THE COURT: Yes.	
16 A. For the purposes of what I was trying to do here, I was			16 MR. JACKSON: Your Honor, she's been an	
17 trying to show an example so when I was explaining something			17 extraordinarily diligent juror, we're very appreciative, but	
18 complex, people could see what things are supposed to look			18 we're happy to have her excused at this point.	
19 like. So didn't explore any of that, no.			19 MR. McRAE: Agreed, your Honor.	
20 Q. And you don't know Steve Maiden, right?			20 MR. WILLIAMS: Your Honor, I think before the defense	
21 A. I saw him, he was called as a witness at a prior hearing,			21 had some suggestion to swapping her as an alternate.	
22 but other than that, no, I never met him.			22 Mr. Jackson made that proposal.	
23 Q. You never worked with him?			23 MR. JACKSON: My suggestion about that was dependent	
24 A. No.			24 on my hope that we would be able to conclude the case by today,	
25 Q. You don't know what he did with the emails that are missing			25 which if we had gotten through summations I think we could have	
HCKTTUZ5		Page 6642	HCKTTUZ5	Page 6644
1 from January 30 to March 10, right?			1 substituted her as an alternate and not released, but since	
2 A. I have no idea.			2 she's not going to hear the end of the case, I think it would	
3 MR. JACKSON: No further questions of this witness.			3 be very difficult to use her.	
4 MS. GRISWOLD: One question for redirect, your Honor?			4 THE COURT: There's no way we could continue with her.	
5 THE COURT: Yes.			5 The only way we could have tried to hold onto her in the form	
6 REDIRECT EXAMINATION			6 of an alternate is if the trial had been completed except for	
7 BY MS. GRISWOLD:			7 deliberations. It hasn't, so there's nothing I can do about	
8 Q. Special Agent DeCapua, did any of the questions that			8 preserving her role on the jury. It's just impossible.	
9 Mr. Jackson just asked you change any of the opinions that you			9 MR. WILLIAMS: We understand, we don't object to her	
10 offered in your direct testimony?			10 being removed.	
11 A. No.			11 THE COURT: All right. So that at the close of the	
12 MS. GRISWOLD: No further questions.			12 day, Mr. Ruocco, I ask you if you could bring Ms. Charlton out	
13 THE COURT: Anything else, sir?			13 so we could all express our appreciation to her and tell her	
14 MR. JACKSON: No, Judge.			14 that she is excused. So we'll do that at the end of the day.	
15 THE COURT: You can step down.			15 MR. McRAE: Your Honor, what was the juror number of	
16 The government may call its next witness.			16 the first person, the first note you described?	
17 MS. GRISWOLD: The government calls Stephen Maiden,			17 THE COURT: This is a man we heard from recently, Eric	
18 but we might need a minute, your Honor, to make sure the			18 Eleam. He sent out a note about an issue, I think it was last	
19 marshals bring him up.			19 week. He's alternate number three, Mr. Ruocco informs me.	
20 THE COURT: All right. So should we take a brief			20 So you want to think about what we should do about	
21 recess?			21 Mr. Eleam?	
22 MS. GRISWOLD: If we could, your Honor.			22 MR. WILLIAMS: Your Honor, we would suggest right now	
23 THE COURT: Ladies and gentlemen, we'll have a take a			23 that we get some more information from him potentially	
24 brief recess.			24 including the nature of this training. Every employer,	
25 (Continued on next page)			25 presumably, certainly the government, have online trainings	